

Commands for the Catalyst 6500 Series Switch WebVPN Module

This chapter contains an alphabetical listing of commands for the Catalyst 6500 series WebVPN Module.

For additional WebVPN Services Module information, refer to the following documentation:

- · Catalyst 6500 Series Switch WebVPN Services Module Installation and Verification Note
- Catalyst 6500 Series Switch WebVPN Services Module Configuration Note
- Catalyst 6500 Series Switch WebVPN Services Module System Message Guide

clear webvpn nbns

To reset the NetBIOS name service (NBNS) cache on the WebVPN Services Module, use the **clear webvpn nbns** command.

clear webvpn nbns [context {name | all}]

Syntax Description

context	(Optional) Clears the statistics for a specific context.
name	Specifies the name of the context.
all	Specifies all contexts.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

To reset all the statistics counters that the WebVPN Services Module maintains, use the **clear webvpn nbns** command without options.

Examples

This example shows how to reset the statistics counters that are maintained in the different system components on the WebVPN Services Module:

webvpn# clear webvpn nbns context context1

clear webvpn platform

To reset the platform extensions on the WebVPN Services Module, use the **clear webvpn platform** command.

clear webvpn platform {conn | session | stats [type] | tunnel stats}

Syntax Description

conn	Clears global connection.
session	Clears session information.
stats	Clears statistics information.
type	(Optional) See the "Usage Guidelines" for available options.
tunnel stats	Clears tunnel counters.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The available options for **stats** type are as follows:

- **crypto**—Clears crypto statistics information.
- crypto module module—Clears crypto statistics for the specified module type.
- fdu—Clears FDU statistics information.
- **ipc**—Clears IPC statistics information.
- **ipc module**—Clears IPC statistics for the specified module type.
- **module** *module*—Clears statistics for the specified module type.

The available options for the module variable are as follows:

- all—All CPUs
- **fdu**—FDU CPU
- ssl1—SSL1 CPU
- tcp1—TCP1 CPU
- tcp2—TCP2 CPU

• **pki** [pki_type]—Clears PKI statistics information.

The available options for the *pki_type* variable are as follows:

- **auth**—Certificate authentication and authorization statistics.
- **cache**—Peer certificate cache statistics.
- **cert-header**—Certificate header insertion statistics.
- **expiring**—Certificate expiration warning statistics.
- **ipc**—Interprocessor communication statistics.
- memory—Memory usage statistics.
- **pki module**—Clears PKI statistics for the specified module type.
- ssl—Clears SSL statistics information.
- tcp—Clears TCP statistics information.

Examples

This example shows how to reset the platform counters that are maintained in the different system components on the WebVPN Services Module:

webvpn# clear webvpn platform

clear webvpn session

To clear the WebVPN session, use the clear webvpn session command.

clear webvpn session {context {name | all} | user name {context {name | all}}}}

Syntax Description

context	Clears the statistics for a specific context.
name	Specifies the name of the context.
all	Specifies all contexts.
user name	Specifies the user name.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

To reset all the statistics counters that the WebVPN Services Module maintains, use the **clear webvpn nbns** command without options.

Examples

This example shows how to reset the session counters that are maintained in the different system components on the WebVPN Services Module:

webvpn# clear webvpn session

clear webvpn stats

To reset the statistics counters that are maintained in the different system components on the WebVPN Services Module, use the **clear webvpn stats** command.

clear webvpn stats [cifs [context {name | all}] | context {name | all} | mangle [context {name | all}] | port-forward [context {name | all}] | tunnel [context {name | all}]]

Syntax Description

cifs	(Optional) WebVPN CIFS statistics
context	(Optional) Clears the statistics for a specific context.
name	(Optional) Specifies the name of the context.
all	(Optional) Specifies all contexts.
mangle	(Optional) Clears the WebVPN mangling statistics.
port-forward	(Optional) Clears the WebVPN port-forwarding statistics.
tunnel	(Optional) Clears the WebVPN tunnel statistics.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

To reset all the statistics counters that the WebVPN Services Module maintains, use the **clear ssl-proxy stats** command without options.

Examples

This example shows how to reset the statistics counters that are maintained in the different system components on the WebVPN Services Module:

```
webvpn# clear webvpn stats cifs
webvpn# clear webvpn stats context context1
webvpn# clear webvpn stats mangle context all
webvpn# clear webvpn stats tunnel
```

This example shows how to clear all the statistic counters that the WebVPN Services Module maintains:

```
webvpn# clear webvpn stats
webvpn#
```

crypto key export rsa pem

To export a PEM-formatted RSA key to the WebVPN Services Module, use the **crypto key export rsa pem** command.

crypto key export rsa *keylabel* **pem** {**terminal** | **url** *url*} {{3des | des} *pass_phrase*}

Syntax Description

keylabel	Name of the key.
terminal	Displays the request on the terminal.
url url	Specifies the URL location. Valid values for <i>url</i> are as follows:
	• archive:—Exports to archive: file system
	• flash:—Exports to flash: file system
	• ftp:—Exports to ftp: file system
	• http:—Exports to http: file system
	• https:—Exports to https: file system
	• null:—Exports to null: file system
	• nvram:—Exports to nvram: file system
	• rcp:—Exports to rcp: file system
	• scp:—Exports to scp: file system
	• system: —Exports to system: file system
	• tftp:—Exports to tftp: file system
3des	Specifies the 168-bit DES (3DES) encryption algorithm.
des	Specifies the 56-bit DES-CBC encryption algorithm.
pass_phrase	Pass phrase.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
WebVPN Services Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The pass phrase can be any phrase including spaces and punctuation except for a question mark (?), which has special meaning to the Cisco IOS parser.

Pass-phrase protection associates a pass phrase with the key. The pass phrase is used to encrypt the key when it is exported. When this key is imported, you must enter the same pass phrase to decrypt it.

Examples

This example shows how to export a key from the WebVPN Services Module:

```
wwbvpn(config)# crypto key export rsa test-keys pem url scp: 3des password
% Key name:test-keys
   Usage:General Purpose Key
Exporting public key...
Address or name of remote host []? 7.0.0.7
Destination username [ssl-proxy]? lab
Destination filename [test-keys.pub]?
Password:
Writing test-keys.pub Writing file to scp://lab@7.0.0.7/test-keys.pub
Password:
Exporting private key...
Address or name of remote host []? 7.0.0.7
Destination username [ssl-proxy]? lab
Destination filename [test-keys.prv]?
Password:
Writing test-keys.prv Writing file to scp://lab@7.0.0.7/test-keys.prv
Password:
wwbvpn(config)#
```

crypto key generate

To generate RSA key pairs, use the **crypto key generate** command.

crypto key generate rsa {usage-keys|general-keys| {label key-label| [exportable] [modulus size]

Syntax Description

general-keys	Generate a general purpose RSA key pair for signing and encryption
usage-keys	Generate seperate RSA key pairs for signing and encryption
label key-label	Specifies the key.
exportable	(Optional) Specifies that the key is allowed to be exported.
modulus size	(Optional) Specifies the modulus length in bits; valid values are 512, 768, 1024, 1536, and 2048 bits. See the "Usage Guidelines" section for more information.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
WebVPN Services Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The WebVPN Services Module supports up to eight levels of certificate authority (one root certificate authority and up to seven subordinate certificate authorities).

You can specify that a key is exportable during key generation. Once the key is generated as either exportable or not exportable, it cannot be modified for the life of the key.



The WebVPN Services Module supports modulus lengths of 512, 768, 1024, 1536, and 2048 bits. Although you can specify 512 or 768, we recommend a minimum modulus length of 1024. A longer modulus takes longer to generate and takes longer to use, but it offers better security.

After you generate a key pair, you can test the SSL service by generating a self-signed certificate.

Examples

This example shows how to generate special-usage RSA keys:

crypto key generate rsa usage-keys

The name for the keys will be: myrouter.example.com

Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.

Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus[512]? <return>

Generating RSA keys.... [OK].

Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus[512]? <return>

Generating RSA keys.... [OK].

This example shows how to generate general-purpose RSA keys:



You cannot generate both special-usage and general-purpose keys; you can generate only one or the other.

webvpn(config)# crypto key generate rsa general-keys label kp1 exportable

The name for the keys will be: kp1

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024 Generating RSA keys.... [OK].

crypto key import rsa pem

To import a PEM-formatted RSA key from an external system, use the **crypto key import rsa pem** command.

crypto key import rsa keylabel pem [usage-keys] {terminal | url url} [exportable] passphrase}

Syntax Description

keylabel	Name of the key.	
usage-keys	(Optional) Specifies that two special-usage key pairs should be generated, instead of one general-purpose key pair.	
terminal	Displays the request on the terminal.	
url url	Specifies the URL location. Valid values are as follows:	
	• archive:—Imports from archive: file system.	
	• cns:—Imports from cns: file system.	
	• flash:—Imports from flash: file system.	
	• ftp:—Imports from ftp: file system.	
	• http:—Imports from http: file system.	
	• https:—Imports from https: file system.	
	• null: —Imports from null: file system.	
	• nvram:—Imports from nvram: file system.	
	• rcp:—Imports from rcp: file system.	
	• scp:—Imports from scp: file system.	
	• system:—Imports from system: file system.	
	• tftp:—Imports from tftp: file system.	
exportable	(Optional) Specifies that the key can be exported.	
passphrase	Pass phrase.	

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
WebVPN Services Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The pass phrase can be any phrase including spaces and punctuation except for a question mark (?), which has special meaning to the Cisco IOS parser.

Pass-phrase protection associates a pass phrase with the key. The pass phrase is used to encrypt the key when it is exported. When this key is imported, you must enter the same pass phrase to decrypt it.

Examples

This example shows how to import a PEM-formatted RSA key from an external system and export the PEM-formatted RSA key to the WebVPN Services Module:

```
wwbvpn(config)# crypto key import rsa newkeys pem url scp: password
% Importing public key or certificate PEM file...
Address or name of remote host []? 7.0.0.7
Source username [ssl-proxy]? lab
Source filename [newkeys.pub]? test-keys.pub
Password:
Sending file modes: C0644 272 test-keys.pub
Reading file from scp://lab@7.0.0.7/test-keys.pub!
% Importing private key PEM file...
Address or name of remote host []? 7.0.0.7
Source username [ssl-proxy]? lab
Source filename [newkeys.prv]? test-keys.prv
Password:
Sending file modes:C0644 963 test-keys.prv
Reading file from scp://lab@7.0.0.7/test-keys.prv!% Key pair import succeeded.
wwbvpn(config)#
```

crypto pki authenticate

To obtain the certificate that contains the public key of the certificate authority, use the **crypto pki** authenticate command.

crypto pki authenticate trustpoint-label

S١	/ntax	Descri	ption

trustpoint-label	Name of th	ne trustpoint label.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
WebVPN Module	Support for this command was introduced on the Catalyst 6500 series
Release 1.1	switches.

Usage Guidelines

The trustpoint-label argument is case-sensitive.

For each trustpoint, you must obtain a certificate that contains the public key of the certificate authority; multiple trustpoints can use the same certificate authority.



Contact the certificate authority to obtain the correct fingerprint of the certificate and verify the fingerprint displayed on the console.

Examples

This example shows how to obtain the certificate of the certificate authority:

webvpn(config)# crypto pki authenticate PROXY1
Certificate has the following attributes:
Fingerprint: A8D09689 74FB6587 02BFE0DC 2200B38A
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
webvpn(config)# end
webvpn#

crypto pki certificate

To configure and define the PKI implementation on the WebVPN Services Module, use the **crypto pki certificate** command.

crypto pki certificate {chain name | map map_name | query | validate trustpoint-label}

Syntax Description

chain	Identifies certificates.	
name	CA server name.	
map	Defines certificate attributes map.	
map_name	CA map tag name.	
query	y Obtains certificates from the CA after reboot.	
validate	e Validates a certificate chain.	
trustpoint-label	Trustpoint label name.	

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The **crypto pki certificate chain** command puts you into certificate chain configuration mode. When you are in certificate chain configuration mode, you can delete certificates using the certificate command. You need to be in certificate chain configuration mode to delete certificates.

The **crypto pki certificate validate** command validates the router's own certificate for a given trustpoint. Use this command as a sanity check after enrollment to verify that the trustpoint is properly authenticated, a certificate has been requested and granted for the trustpoint, and that the certificate is currently valid. A certificate is valid if it is signed by the trustpoint certification authority (CA), not expired, and so on.

crypto pki crl request

To configure and define the PKI implementation on the WebVPN Services Module, use the **crypto pki crl request** command.

crypto pki crl request name

S١	/ntax	Descri	ption

name	Specifies the name of the CA. This is the same name used when the CA was
	declared with the crypto pki trustpoint command.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

A CRL lists all the certificates of the network device that have been revoked. Revoked certificates will not be honored by your module; therefore, any IPSec device with a revoked certificate cannot exchange IP Security traffic with your module.

The first time your module receives a certificate from a peer, it will download a CRL from the CA. Your module then checks the CRL to make sure the certificate of the peer has not been revoked. (If the certificate appears on the CRL, it will not accept the certificate and will not authenticate the peer.)

A CRL can be reused with subsequent certificates until the CRL expires. If your module receives the certificate of a peer after the applicable CRL has expired, it will download the new CRL.

If your module has a CRL which has not yet expired, but you suspect that the contents of the CRL are out of date, use the **crypto pki crl request** command to request that the latest CRL be immediately downloaded to replace the old CRL.

This command is not saved to the configuration.

Examples

This example shows how to specify the timeout in seconds for each request:

wwbvpn(config)# crypto pki crl request

crypto pki enroll

To request a certificate for the trustpoint, use the crypto pki enroll command.

crypto pki enroll trustpoint-label

Syntax Description

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The trustpoint-label argument is case-sensitive.

You must obtain a signed certificate from the certificate authority for each trustpoint.

You have the option to create a challenge password that is not saved with the configuration. This password is required if your certificate needs to be revoked, so you must remember this password.



If your module or switch reboots after you have entered the crypto **pki enroll** command, but before you have received the certificates, you must reenter the command and notify the certificate authority administrator.

Examples

This example shows how to request a certificate:

```
webvpn(config)# crypto pki enroll PROXY1
%
    Start certificate enrollment..
% The subject name in the certificate will be: C=US; ST=California; L=San Jose; O=Cisco;
OU=Lab; CN=hostl.cisco.com
% The subject name in the certificate will be: host.cisco.com
% The serial number in the certificate will be: 00000000
% The IP address in the certificate is 10.0.0.1
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.
Fingerprint: 470DE382 65D8156B 0F84C2AF 4538B913
webvpn(config)# end
```

crypto pki export pem

To export privacy-enhanced mail (PEM) files from the WebVPN Services Module, use the **crypto pki export pem** command.

crypto pki export trustpoint_label pem {terminal {des | 3des} {url url}} pass_phrase

Syntax Description

trustpoint-label	Name of the trustpoint.
terminal	Displays the request on the terminal.
des	Specifies the 56-bit DES-CBC encryption algorithm.
3des	Specifies the 168-bit DES (3DES) encryption algorithm.
url url	Specifies the URL location. Valid values for <i>url</i> are as follows:
	• archive:—Exports to archive: file system
	• flash:—Exportsto flash: file system
	• ftp:—Exports to the FTP: file system
	• http:—Exports to HTTP: file system
	• https:—Exports to HTTPS: file system
	• null:—Exports to the NULL: file system
	 nvram:—Exports to the NVRAM: file system
	• rcp:—Exports to the RCP: file system
	• scp:—Exports to the SCP: file system
	• system:—Exports to the system: file system
	• tftp:—Exports to the TFTP: file system
pass-phrase	Pass phrase that is used to protect the private key.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
WebVPN Services Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The *pass_phrase* can be any phrase including spaces and punctuation except for a question mark (?), which has special meaning to the Cisco IOS parser.

Pass-phrase protection associates a pass phrase with the key. The pass phrase is used to encrypt the key when it is exported. When this key is imported, you must enter the same pass phrase to decrypt it.

A key that is marked as unexportable cannot be exported.

You can change the default file extensions when prompted. The default file extensions are as follows:

- public key (.pub)
- private key (.prv)
- certificate (.crt)
- CA certificate (.ca)
- signature key (-sign)
- encryption key (-encr)

Examples

This example shows how to export a PEM-formatted file on the WebVPN Services Module:

wwbvpn(config)# crypto pki export TP5 pem url tftp://10.1.1.1/TP5 password

Related Commands

crypto pki import pem

crypto pki export pkcs12

To export a PKCS12 file from the WebVPN Services Module, use the **crypto pki export pkcs12** command.

crypto pki export trustpoint_label **pkcs12** file_system [pkcs12_filename] pass_phrase

Syntax Description	trustpoint_label	Specifies the trustpoint label.
	file_system	Specifies the file system. Valid values for file_system are as follows
		archive:—Exports to archive: file system.
		cns:—Exports to cns: file system.
		flash:—Exports to flash: file system.
		ftp:—Exports to ftp: file system.
		http:—Exports to http: file system.
		https:—Exports to https: file system.
		null:—Exports to null: file system.
		nvram:—Exports to nvram: file system.
		rcp:—Exports to rcp: file system.
		scp:—Exports to scp: file system.
		system:—Exports to system: file system.
		terminal—Outputs the PKCS12 file to the terminal.
		tftp:—Exports to tftp: file system.
	pkcs12_filename	(Optional) Specifies the name of the PKCS12 file to import.
	pass_phrase	Specifies the pass phrase of the PKCS12 file.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
WebVPN Module	Support for this command was introduced on the Catalyst 6500 series
Release 1.1	switches.

Usage Guidelines

Imported key pairs cannot be exported.

If you are using SSH, we recommend using SCP (secure file transfer) when exporting a PKCS12 file. SCP authenticates the host and encrypts the transfer session.

If you do not specify the *pkcs12_filename* value, you will be prompted to accept the default filename (the default filename is the *trustpoint_label* value) or enter the filename. For the **ftp:** or **tftp:** value, include the full path in the *pkcs12_filename* value.

You will receive an error if you enter the pass phrase incorrectly.

If there is more than one level of CA, the root CA and all the subordinate CA certificates are exported in the PKCS12 file.

Examples

This example shows how to export a PKCS12 file using SCP:

```
wwbvpn(config)# crypto ca export TP1 pkcs12 scp: sky is blue
Address or name of remote host []? 10.1.1.1
Destination username [ssl-proxy]? admin-1
Destination filename [TP1]? TP1.p12

Password:
Writing TP1.p12 Writing pkcs12 file to scp://admin-1@10.1.1.1/TP1.p12

Password:
!
CRYPTO_PKI:Exported PKCS12 file successfully.
wwbvpn(config)#
```

crypto pki import pem

To import a PEM-formatted file to the WebVPN Services Module, use the **crypto pki import pem** command.

trustpoint-label	Name of the trustpoint.	
exportable	(Optional) Specifies the key that can be exported.	
terminal	Displays the request on the terminal.	
url url	Specifies the URL location. Valid values for <i>url</i> are as follows:	
	• archive:—Imports from archive: file system.	
	• flash:—Imports from flash: file system.	
	• ftp: —Imports from the FTP: file system.	
	• http:—Importsfrom HTTP: file system.	
	• https:—Imports from HTTPS: file system.	
	• null:—Imports from the NULL: file system.	
	• nvram:—Imports from the NVRAM: file system.	
	• rcp:—Imports from the RCP: file system.	
	• scp:—Imports from the SCP: file system.	
	• system:—Imports from the system: file system.	
	• tftp:—Imports from the TFTP: file system.	
usage-keys	Specifies that two special-usage key pairs should be generated, instead of one general-purpose key pair.	
pass_phrase	Pass phrase.	

Defaults

This command has no default settings.

Command History

Global configuration

Command History

Release	Modification
WebVPN Services	Support for this command was introduced on the Catalyst 6500 series
Module Release 1.1	switches.

Usage Guidelines

You will receive an error if you enter the pass phrase incorrectly. The pass phrase can be any phrase including spaces and punctuation except for the question mark (?), which has special meaning to the Cisco IOS parser.

Pass-phrase protection associates a pass phrase with the key. The pass phrase is used to encrypt the key when it is exported. When this key is imported, you must enter the same pass phrase to decrypt it.

When importing RSA keys, you can use a public key or its corresponding certificate.

The **crypto ca import pem** command imports only the private key (.prv), the server certificate (.crt), and the issuer CA certificate (.ca). If you have more than one level of CA in the certificate chain, you need to import the root and subordinate CA certificates before this command is used for authentication. Use the cut-and-paste feature or TFTP to import the root and subordinate CA certificates.

Examples

This example shows how to import a PEM-formatted file from the WebVPN Services Module:

```
wwbvpn(config)# crypto pki import TP5 pem url tftp://10.1.1.1/TP5 password
% Importing CA certificate...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.ca]?
Reading file from tftp://10.1.1.1/TP5.ca
Loading TP5.ca from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1976 bytes]
% Importing private key PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.prv]?
Reading file from tftp://10.1.1.1/TP5.prv
Loading TP5.prv from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 963 bytes]
% Importing certificate PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.crt]?
Reading file from tftp://10.1.1.1/TP5.crt
Loading TP5.crt from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1692 bytes]
% PEM files import succeeded.
wwbvpn(config)# end
*Apr 11 15:11:29.901: %SYS-5-CONFIG_I: Configured from console by console
```

Related Commands

crypto pki export pem

crypto pki import pkcs12

To import a PKCS12 file to the WebVPN Services Module, use the crypto ca import pkcs12 command.

crypto pki import trustpoint_label pkcs12 file_system [pkcs12_filename] pass_phrase

Syntax Description	trustpoint_label	Specifies the trustpoint label.
	file_system	Specifies the file system. Valid values for <i>file_system</i> are as follows:
		archive:—Exports to archive: file system.
		cns:—Exports to cns: file system.
		flash:—Exports to flash: file system.
		ftp:—Exports to ftp: file system.
		http:—Exports to http: file system.
		https:—Exports to https: file system.
		null:—Exports to null: file system.
		nvram:—Exports to nvram: file system.
		rcp:—Exports to rcp: file system.
		scp:—Exports to scp: file system.
		system:—Exports to system: file system.
		terminal—Outputs the PKCS12 file to the terminal.
		tftp:—Exports to tftp: file system.
	pkcs12_filename	(Optional) Specifies the name of the PKCS12 file to import.
	pass_phrase	Specifies the pass phrase of the PKCS12 file.
	-	

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

If you are using SSH, we recommend using SCP (secure file transfer) when importing a PKCS12 file. SCP authenticates the host and encrypts the transfer session.

If you do not specify a value for *pkcs12_filename*, you will be prompted to accept the default filename (the default filename is the *trustpoint_label* value) or to enter the filename. For the **ftp:** or **tftp:** value, include the full path in the *pkcs12_filename* value.

You will receive an error if you enter the pass phrase incorrectly.

If there is more than one level of CA, the root CA and all the subordinate CA certificates are exported in the PKCS12 file.

Examples

This example shows how to import a PKCS12 file using SCP:

```
wwbvpn(config)# crypto ca import TP2 pkcs12 scp: sky is blue
Address or name of remote host []? 10.1.1.1
Source username [ssl-proxy]? admin-1
Source filename [TP2]? /users/admin-1/pkcs12/TP2.p12

Password:password
Sending file modes:C0644 4379 TP2.p12
!
wwbvpn(config)#
*Aug 22 12:30:00.531:%CRYPTO-6-PKCS12IMPORT_SUCCESS:PKCS #12 Successfully Imported.
wwbvpn(config)#
```

Global configuration

crypto pki profile enrollment

To define an enrollment profile, use the **crypto pki profile enrollment** command in global configuration mode. To delete all information associated with this enrollment profile, use the **no** form of this command.

crypto pki profile enrollment label

Syntax Description	label	Certificate enrollment profile tag.
Defaults	This command	has no default settings.

Command History

Command Modes

Release	Modification
WebVPN Module	Support for this command was introduced on the Catalyst 6500 series
Release 1.1	switches.

Usage Guidelines

After entering the **crypto pki profile enrollment** command, you can use any of the following commands to define the profile parameters:

- **authentication command**—Specifies the HTTP command that is sent to the certification authority (CA) for authentication.
- authentication terminal—Specifies manual cut-and-paste certificate authentication requests.
- authentication url—Specifies the URL of the CA server to which to send authentication requests.
- enrollment command—Specifies the HTTP command that is sent to the CA for enrollment.
- enrollment terminal—Specifies manual cut-and-paste certificate enrollment.
- enrollment url—Specifies the URL of the CA server to which to send enrollment requests.
- **parameter**—Specifies parameters for an enrollment profile. This command can be used only if the authentication command or the enrollment command is used.



The authentication url, enrollment url, authentication terminal, and enrollment terminal commands allow you to specify different methods for certificate authentication and enrollment, such as TFTP authentication and manual enrollment.

Examples

This example shows how to specify the timeout in seconds for each request:

webvpn(config)# crypto pki profile enrollment test
webvpn(ca-profile-enroll)#

crypto pki trustpoint

To enter the configuration submode for the certificate-authority trustpoint and define the certificate-authority trustpoint, use the **crypto pki trustpoint** command. Use the **no** form of this command to remove any commands that you have entered in the WebVPN subcommand mode from the configuration.

crypto pki trustpoint trustpoint-label

no crypto pki trustpoint trustpoint-label

	Syntax Description to	rustpoint-label	(Optional) Name of the trustpoint label.
--	-----------------------	-----------------	--

Defaults This command has no default settings.

Command Modes Global configuration

Command History Release WebVPN Module Release 1.1 Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines The *trustpoint-label* argument is case-sensitive.

After you enter the **crypto pki trustpoint** command, the prompt changes to the following:

webvpn(ca-trustpoint)#

After you enter the ca-trustpoint submode, there are commands available to configure the CA trustpoint. Table 2-1 lists the ca-trustpoint submode commands.

Table 2-1 Certificate-Authority Trustpoint Submode Commands

Command	Purpose and Guidelines	Defaults
authorization {list listname username	Authorization parameters.	
{subjectname subjectname}}	list <i>listname</i> —Specifies the AAA authorization list.	
	username subjectname subjectname—Sets parameters for the different certificate fields that are used to build the AAA username.	
	The following are options that may be used as the AAA username:	
	• commonname—Certificate common name.	
	• country—Certificate country.	
	email—Certificate email.	
	• ipaddress—Certificate IP address.	
	locality—Certificate locality.	
	• organization—Certificate organization.	
	• organizationalunit—Certificate organizational unit.	
	• postalcode —Certificate postal code.	
	• serialnumber—Certificate serial number.	
	• state—Certificate state field.	
	• streetaddress —Certificate street address.	
	• title—Certificate title.	
	• unstructuredname —Certificate unstructured name.	
auto-enroll [[value] regenerate]]	Automatically enrolls this router identity.	
	regenerate —(Optional) A new key is generated for the certificate even if the named key already exists.	
	<i>value</i> = 1–100	
crl query url		
default	Sets a command to its defaults.	

Table 2-1 Certificate-Authority Trustpoint Submode Commands (continued)

Command	Purpose and Guidelines	Defaults
enrollment [http-proxy][mode ra] [retry {period minutes count count}] url url	Specifies the enrollment parameters for your certificate authority as follows: • http-proxy—HTTP proxy server for enrollment. • mode ra—Registration authority mode. • retry count count— How many times to poll the CA for the certificate; valid values for count are 1 to 100. • retry period minutes—How long to wait between requests to the CA for the certificate; valid values for minutes are 1 to 60. • url url—A URL or one of the following: - archive:—Enrolls using archive: file system. - flash:—Enrolls using flash: file system. - http:—Enrolls using http: file system.	period minutes—1 count count—10
	- ftp: —Enrolls using ftp: file system.	
exit	Exits the ca-trustpoint configuration mode.	
fqdn {fqdn none}	Includes the fully qualified domain name. fqdn—Enter the fully qualified domain name. none—Do not include the fully qualified domain name.	
ip-address server-ip-addr	(Optional) Specifies the IP address of the WebVPN gateway that will use this certificate.	

Table 2-1 Certificate-Authority Trustpoint Submode Commands (continued)

Command	Purpose and Guidelines	Defaults		
match certificate map_name [map override skip]	Associates a certificate-based access control list (ACL) defined with the crypto pki certificate map command.			
	map_name—Matches the map_name argument specified in a previously defined crypto pki certificate map map_name command.			
	allow —Allows expired certificates to be accepted.			
	override—Overrides fields in a certificate.			
	skip—Skips a certificate validity check.			
no	Negates a command or set its defaults.			
ocsp url url	Enters Online Certificate Status Protocol (OCSP) parameters.			
	<i>url</i> —All certificates associated with a configured trustpoint will be checked by the OCSP server at the specified HTTP URL.			
password password	(Optional) Configures a challenge password.			
primary	Specifies the trustpoint as primary.			
query certificate	Turns on query mode per specified trustpoint, causing certificates not to be stored locally and to be retrieved from a remote server.			
rsakeypair key-label	Specifies the key pair to associate with the certificate.			
regenerate	Regenerates keys on reenrollment.			
revocation-check {crl none ocsp}	(Optional) Specifies how this trustpoint looks up a certificate revocation list when validating a certificate associated with this trustpoint.			
	crl —Revocation check by CRL.			
	none—Ignore revocation check.			
	ocsp—Revocation check by OCSP.			
root tftp hostname filename	Defines the TFTP protocol to get the root certificate of a given certification authority. This command enables an authenticated root certificate to be stored as a file on the TFTP server.			
serial-number [none]	Specifies whether or not to include serial number.	Not included		
show	Shows this router trustpoint.			
source interface interface-name	Specifies the address of an interface to be used as the source address for all outgoing TCP connections associated with a trustpoint.			
	interface-name—Interface address to be used as the source address.			

Table 2-1 Certificate-Authority Trustpoint Submode Commands (continued)

Command	Purpose and Guidelines	Defaults
subject-name line	(Optional) Configures the host name of the WebVPN gateway.	
usage {ike ssl-client ssl-server}	(Optional) Specifies the intended use for the certificate.	
vrf vrf	Name of the VPN routing and forwarding instance (VRF) to use for enrollment and obtaining CRLs.	

You should declare one trustpoint to be used by the module for each certificate.

The *trustpoint-label* value should match the *key-label* value of the keys; however, this is not a requirement.

When you specify the IP address of the WebVPN gateway that will use this certificate, some web browsers compare the IP address in the SSL server certificate with the IP address that might appear in the URL. If the IP addresses do not match, the browser may display a dialog box and ask the client to accept or reject this certificate.

When specifying the **subject-name** *line* value, use these guidelines:

- The subject-name command uses the Lightweight Directory Access Protocol (LDAP) format.
- Arguments specified in the subject name must be enclosed in quotation marks if they contain a comma. For example, O="Cisco, Inc."
- Some browsers compare the common name (CN) field of the subject name in the SSL server certificate with the hostname that might appear in the URL. If the names do not match, the browser may display a dialog box and ask the client to accept or reject the certificate. Also, some browsers will reject the SSL session setup and close the session if the CN field is not defined in the certificate.

Examples

This example shows how to declare the trustpoint PROXY1 and verify connectivity:

```
webvpn(config)# crypto pki trustpoint PROXY1
webvpn(ca-trustpoint)# rsakeypair PROXY1
webvpn(ca-trustpoint)# enrollment url http://exampleCA.cisco.com
webvpn(ca-trustpoint)# ip-address 10.0.0.1
webvpn(ca-trustpoint)# password password
webvpn(ca-trustpoint)# serial-number
webvpn(ca-trustpoint)# subject-name C=US; ST=California; L=San Jose; O=Cisco; OU=Lab;
CN=host1.cisco.com
webvpn(ca-trustpoint)# end
webvpn(ca-trustpoint)# end
webvpn# ping example.cisco.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
webvpn#
```

debug webvpn

To turn on the debug flags in different system components, use the **debug webvpn** command. Use the **no** form of this command to turn off the debug flags.

debug webvpn [aaa | cifs | cookie | dns | emweb | http | package | platform [type] | port-forward | sock | timer | trie | tunnel | webservice]

Syntax Description

aaa	Enables WebVPN AAA debugs.
cifs	Enables WebVPN CIFS.
cookie	Enables WebVPN cookie debugs.
dns	Enables DNS debugs.
emweb	Enables EmWeb debugs.
http	Enables HTTP debugs.
package	Enables package debugs.
platform type	See the "Usage Guidelines" for information on the platform <i>type</i> option.
port-forward	Enables port-forward debugs.
sock	Enables socks debugs.
timer	Enables timer debugs.
trie	Enables trie debugs.
tunnel	Enables tunnel debugs.
webservice	Enables web service debugs.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines



For the following options, **module** has the following values:

- fdu—FDU CPU
- ssl1—SSL1 CPU
- tcp1—TCP1 CPU
- tcp2—TCP2 CPU

The **platform** *type* has the following options:

The platform app includes the following values:

- **app** [**module** [*module*]]—App Record Layer
- hdr [module [module]]—App HTTP Header Insertion
- **module** [module]—Module to be debugged
- **url** [**module** [module]]—App URL Rewrite

The **platform app-driver** includes the following values:

- dispatch—Dispatch events
- error—Error events
- event {app | next-hop | tcp}—Event debugging
- fsm—FSM
- mc—Multi-core events

The platform content includes the following values:

- **detail** [module [module]]—Content detail
- **error** [**module** [*module*]]—Content error
- ipc [module [module]]—Content IPC
- module [module]—Module to be debugged
- **rewriting** [**module** [*module*]]—Content rewriting
- scanning [module [module]]—Content scanning

The **platform fdu** includes the following values:

- cli [module [module]]—FDU CLI
- hash [module [module]]—FDU hash
- **ipc** [**module** [module]]—FDU IPC
- **module** [module]—Module to be debugged
- trace [module [module]]—FDU trace

The platform flash includes the following values:

- **module** [module]—Module to be debugged

The **platform ipc** includes the following values:

- **module** [module]—Module to be debugged

The **platform pc** includes the following values:

- **module** [module]—Module to be debugged

The **platform pki** includes the following values:

- auth—Certificate authentication and authorization
- ca-pool—CA Pool
- cert—Certificate management
- events—Events
- history—Certificate history
- ipc—IPC messages and buffers
- **key**—Key management

The **platform remote** includes the following values:

- loop count [module [module]]—Remote debug. Valid values for count are from 1 to 65535.
- **module** [module]—Module to be debugged

The **platform ssl** keyword includes the following values:

- **alert** [**module** [*module*]]—SSL alert events
- **error** [**module** [*module*]]—SSL error events
- handshake [module [module]]—SSL handshake events
- module [module]—Module to be debugged
- pkt [module [module]]—Debugs the received and transmitted SSL packets



Use the TCP debug commands only to troubleshoot basic connectivity issues under little or no load conditions (for instance, when no connection is being established to the virtual server or real server).

If you run TCP debug commands, the TCP module displays large amounts of debug information on the console, which can significantly slow down module performance. Slow module performance can lead to delayed processing of TCP connection timers, packets, and state transitions.

The **platform tcp** keyword includes the following values:

- **events** [**module** [*module*]]—Debugs the TCP events.
- **module** [*module*]—Module to be debugged.
- **pkt** [module [module]]—Debugs the received and transmitted TCP packets.
- state [module [module]]—Debugs the TCP states.
- **timers** [**module** [*module*]]—Debugs the TCP timers.

The platform tunnel keyword includes the following values:

- hash—Tunnel hash entry
- trace—Trace packets for tunnel connection

Examples

This example shows how to turn on tunnel debugging:

```
webvpn# debug webvpn tunnel
webvpn#
```

This example shows how to turn on App debugging:

```
webvpn# debug webvpn platform app
webvpn#
```

This example shows how to turn on FDU debugging:

```
webvpn# debug webvpn platform fdu
webvpn#
```

This example shows how to turn on IPC debugging:

```
webvpn# debug webvpn platform ipc
webvpn#
```

This example shows how to turn on PKI debugging:

```
webvpn# debug webvpn platform pki
webvpn#
```

This example shows how to turn on SSL debugging:

```
 \begin{array}{lll} & ssl\text{-proxy\#} & \textbf{debug webvpn platform ssl} \\ & ssl\text{-proxy\#} \end{array}
```

This example shows how to turn on TCP debugging:

```
 \begin{array}{lll} {\tt ssl-proxy\#} & {\tt debug} & {\tt webvpn} & {\tt platform} & {\tt tcp} \\ {\tt ssl-proxy\#} & & & \\ \end{array}
```

This example shows how to turn off TCP debugging:

```
\verb|ssl-proxy| # no debug webvpn platform tcp \\ \verb|ssl-proxy| # \\
```

do

To execute EXEC-level commands from global configuration mode or other configuration modes or submodes, use the **do** command.

do command

Syntax Description

command	EXEC-level command to be executed.	
---------	------------------------------------	--

Defaults

This command has no default settings.

Command Modes

Global configuration or any other configuration mode or submode from which you are executing the EXEC-level command.

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines



Do not enter the do command in EXEC mode. Interruption of service may occur.

You cannot use the **do** command to execute the **configure terminal** command because entering the **configure terminal** command changes the mode to configuration mode.

You cannot use the **do** command to execute the **copy** or **write** command in the global configuration mode or any other configuration mode or submode.

Examples

This example shows how to execute the EXEC-level **show interfaces** command from within global configuration mode:

wwbvpn(config)# do show interfaces serial 3/0

```
Serial3/0 is up, line protocol is up
  Hardware is M8T-RS232
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output 1d17h, output hang never
  Last clearing of "show interface" counters never
.
.
.
.
.
.
. wwbvpn(config)#
```

nbns-list

To enter the nbnslist submode and configure NetBIOS Name Service (NBNS) servers, use the **nbns-list** command. Use the **no** form of this command to remove the specified list from the configuration.

nbns-list name

no nbns-list name

Sı	/ntax	Descri	intion
_	IIICUA	DC301	Puon

name	Name	for	the	NBNS	list.
TUCTITUC	1 (dille	101	LIIC	112110	IID.

Defaults

This command has no default settings.

Command Modes

WebVPN context submode

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The listname argument is case-sensitive and can be a maximum of 64 characters.

After you enter the **nbns-list** command, the prompt changes to the following:

webvpn(config-webvpn-nbnslist)#

After you enter the nbnslist submode, there are commands available to configure the NBNS servers. Table 2-4 lists the nbnslist submode commands.

Table 2-2 NBNSlist Submode Commands

Command	Purpose and Guidelines	Defaults
nbns-server ip_addr [master] [timeout timeout][retry retries]	Specifies a NetBIOS name service (NBNS) list and server address for common Internet file system (CIFS) name resolution. You can configure up to three servers.	Timeout is 2 seconds. Retries is 2 retries.
	Note Supported only on Windows 2000 and Samba servers running on Linux.	
	The <i>ip_addrs</i> value specifies the primary domain controller (PDC) on a Windows network.	
	The master keyword indicates that this is a master browser. Do not enter the master keyword if this a Windows Internet Naming Service (WINS) server.	
	The <i>timeout</i> value specifies the initial time in seconds to wait for a response to an NBNS query before sending the query to the next server. The default timeout value is 2 seconds; the range is from 1 to 30.	
	The <i>retries</i> value specifies the number of times to retry sending a NBNS query to the configured servers. This value represents the number of times to cycle through the list of servers before returning an error. The default retries value is 2; the range is 0 to 10.	
exit	Returns to context submode.	

Examples

This example shows how to enter the nbnslist submode and configure the NBNS list and server address:

```
webvpn(config)# webvpn context c1
webvpn(config-webvpn-context)# nbns-list list2
webvpn(config-webvpn-nbnslist)# nbns-server 10.1.1.2
webvpn(config-webvpn-nbnslist)# exit
webvpn(config-webvpn-context)#
```

Related Commands

webvpn context

policy group

To define a group-policy template, associate a group-policy with a particular proxy server, and enter the group-policy submode, use the **webvpn policy group** command from context subcommand mode. Use the **no** form of this command to remove any commands that you have entered in the WebVPN subcommand mode from the configuration.

policy group group-policy-name

no policy group group-policy-name

Syntax	Descri	ntion
Jyman	DUSCHI	puon

group-policy-name Name of the group policy.

Defaults

See the "Usage Guidelines" section for the submode command defaults.

Command Modes

WebVPN context submode

Command History

Release	Modification
WebVPN Module	Support for this command was introduced on the Catalyst 6500 series
Release 1.1	switches.

Usage Guidelines

The group-policy-name argument is case-sensitive.

After you enter the **policy group** command, the prompt changes to the following:

webvpn(config-webvpn-group)#

Table 2-3 lists the commands available to configure the group-policy template.

Table 2-3 Group-policy Commands

Command	Purpose and Guidelines	Defaults
banner value string	Specifies the banner string for the user or group. The <i>string</i> value may contain 7-bit ASCII values, HTML tags, and escape sequences. This string is presented to the user after login.	No string is specified.
exit	Exits from group-policy configuration mode.	
filter tunnel {ip-acl ip-expanded-acl name}	 Defines the tunnel-specific access list. ip-acl—IP access list (standard or extended); valid values are from 1 to 199. ip-expanded-acl—IP expanded access list (standard or extended); valid values are from 1300 to 2699. name—Access-list name. 	No name is specified.

Table 2-3 Group-policy Commands

Command	Purpose and Guidelines	Defaults
functions {file-access file-browse file-entry svc-enabled svc-required }	Note You must enable file-access before you can enable file-browse or file-entry.	All values are disabled.
sie requireu;	 file-access—Allows you to access the file servers that are listed on the home page. file-browse—Allows you to browse file servers. When you disable this option, you are denied entry to a file server. file-entry—Allows you to alter a file in a file server. svc-enabled—Allows the user of the group to use tunnel mode. If the SVC fails to install on the end user's PC, the end user can continue to use clientless mode or thin-client mode. svc-required—Tunnel mode is required. If the SVC fails to 	
hide-url-bar	install on the end user's PC, the end user cannot use other modes. Disables the URL bar on the portal page. Note This command applies only to clientless mode.	
nbns-list name	Specifies the NBNS list for CIFS as defined in the context configuration. Supported only with Windows 2000 servers and Linux/UNIX. Note This command applies only to clientless mode.	
no	Negates a command or set its defaults.	
port-forward name	Specifies the port-forward list as defined in the context configuration. Entering the command again overrides the previous setting. The default is to have no list specified, Note This command applies only to thin-client mode.	No list specified, and port forwarding is disabled.
timeout {idle session} seconds	Specifies the end-user idle timeout value and maximum session timeout value for the user or group.	idle seconds—2100 seconds (35 minutes)
	idle seconds—Specifies the end-user inactivity. Valid values for idle timeout are from 0 (disabled) to 3600 seconds.	session seconds—43200 seconds (12 hours)
	session <i>seconds</i> —Specifies the total session time, regardless of activity. Valid values for session timeout are from 1 to 1209600 seconds.	
svc	Specifies the tunnel configuration; see the svc command for additional information.	
url-list name	Specifies the URL list as defined in the context configuration. Entering the command again overrides the previous setting.	No list is specified.
	Note This command applies only to clientless mode.	

Examples

This example show how to configure the WebVPN context and the WebVPN group-policy:

```
webvpn(config)# webvpn context cisco
webvpn(config-webvpn-context)# policy group cisco_tunl
webvpn(config-webvpn-group)# function svc-enabled
webvpn(config-webvpn-group)# timeout idle 36000
webvpn(config-webvpn-group)# timeout session 144000
webvpn(config-webvpn-group)# svc address-pool "cisco_tunl_pool"
webvpn(config-webvpn-group)# svc keep-client-installed
webvpn(config-webvpn-group)# svc rekey time 40000
webvpn(config-webvpn-group)# svc rekey method new-tunnel
webvpn(config-webvpn-group)# svc dpd-interval gateway 0
webvpn(config-webvpn-group)# svc dpd-interval client 300
webvpn(config-webvpn-group)# exit
webvpn(config-webvpn-context)#
```

port-forward

To enter the port-forwarding submode and configure port-forwarding entries, use the **port-forward** command. Use the **no** form of this command to remove the given list from the configuration.

port-forward listname

no port-forward listname

Syntax Description	listname	Name for list of forwarded ports.
Defaults	This command has no	default settings.
Command Modes	WebVPN context sub-	mode
Command History	Release	Modification
	WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.
Usage Guidelines	The <i>listname</i> argumer	nt is case-sensitive and can be a maximum of 64 characters.
After you enter the port-forward command, the prompt changes to the following		ort-forward command, the prompt changes to the following:
	webvpn(config-webvp	on-port-fwd)#
	•	ort-forward submode, there are commands available to configure the ces. Table 2-4 lists the port-forwarding submode commands.

Table 2-4 Port-Forwarding Submode Commands

Command	Purpose and Guidelines	Defaults
default local-port port-number	Specifies the default local port; valid values are from 1 to 65535.	
exit	Exits WebVPN port-fwd submode and returns to WebVPN context submode.	

Table 2-4 Port-Forwarding Submode Commands (continued)

Command	Purpose and Guidelines	Defaults
local localport	Specifies the local port that is listened upon; a <i>localport</i> value may be used only once within a given listname. Valid values are from 1 to 65535. After you specify the local port, the following keywords and arguments are available:	
	• remote-server <i>remoteserver</i> —Specifies the DNS name or IP address to connect to on the remote server.	
	• remote-port <i>remoteport</i> —Specifies the port to connect to on the remote server. Valid values are from 1 to 65535.	
	• description —Specifies an application name or short description to display on the end user applet window. The maximum length of the <i>description</i> value is 64 characters.	
no	Removes the matching line from the configuration.	

You can specify multiple entries for a given *listname* value. The *listname* value is provided to group the port forwarding entries into a list that can be applied to a username or a group policy.

Specifying **no** removes the matching line from the configuration; the remote server and remote port do not need to be included.

Examples

This example shows how to enter the port-forwarding submode and configure port-forwarding entries:

```
webvpn(config-webvpn-context)# port-forward abc
webvpn(config-webvpn-port-fwd)# local-port 25 remote-server "mailman" remote-port 25
description "SMTP server"
webvpn(config-webvpn-port-fwd)# local-port 110 remote-server "pop3-ny" remote-port 110
description "POP3-server"
webvpn(config-webvpn-port-fwd)# local-port 143 remote-server "imap-ny" remote-port 143
description "IMAP server"
webvpn(config-webvpn-port-fwd)#
```

Related Commands

url-list

webvpn context

show webvpn context

To display information about a specific context, use the **show webvpn context** command.

show webvpn context name

Syntax Description name Specifies the name of the context.	Syntax Description	name	Specifies the name of the context.	
--	--------------------	------	------------------------------------	--

Defaults This command has no default settings.

Command Modes EXEC

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to collect information about the software-forced reset:

webvpn# show web context tunnel

Admin Status: up Operation Status: up TCP Policy not configured SSL Policy not configured

Certificate authentication type: peer certificate is always accepted

AAA Authentication List: webvpn

AAA Authentication Domain not configured

Default Group Policy: tunnel Associated WebVPN Gateway: s2

Domain Name and Virtual Host not configured

Maximum Users Allowed: 2560 (default)

NAT Address Range: 10.81.12.4-10.81.12.9 mask 255.255.255.0

VRF Name not configured

show webvpn dispatch

To display WebVPN dispatching information, use the show webvpn dispatch command.

show webvpn dispatch {algorithm | member | stats}

Syntax Description

algorithm	Displays the current content load balancing (CLB) algorithm.
member	Displays CLB member table infomation.
stats	Displays the dispatching statistics.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display the WebVPN dispatching statistics:

This example shows how to display the current CLB algorithm:

This example shows how to display CLB member table infomation:

webvpn# show webvpn dispatch member

SSLVPN: CLB Member Table

(Current RR Index 1):
Member-Index Core-ID

Member-Index	Core-ID	Symbolic-ID	Weight	Quota
0	1	SwCidIos	5	3
1	7	SwCidVpn1	6	2

show webvpn gateway

To display gateway information, use the show webvpn gateway command.

show webvpn gateway [name]

Syntax Description

) Name of the gateway.
) Name of the gateway.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display information for all gateways:

webvpn# show webvpn gateway

Gateway Name	Admin	Operation
s1	up	up
s2	up	up
gateway1	down	down
tunnel	down	down

This example shows how to display information for a specific gateway:

webvpn# show webvpn gateway s1

```
Admin Status: up
Operation Status: up
IP: 10.1.2.140, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: tp1
Certificate chain for new connections:
Certificate:
    Key Label: tp1, 1024-bit, not exportable
    Key Timestamp: 12:09:27 UTC Dec 25 2004
    Serial Number: 0FE5
Root CA Certificate:
    Serial Number: 01
rsa-general-purpose certificate
Certificate chain complete
```

show webvpn install

To display information on installed WebVPN files and packages, use the **show webvpn install** command.

show webvpn install {file filename | package {csd | svc}| status {csd | svc}}

Syntax Description

file	Displays the contents of the file.
filename	Name of the file.
package	Displays the contents of the package.
csd	Specifies the Cisco Secure Desktop (CDP).
svc	Specifies the SSL VPN client (SVC).
status	Displays the status of the package.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module	Support for this command was introduced on the Catalyst 6500 series
Release 1.1	switches.

Examples

This example shows how to display status information about the SSL VPN client (SVC):

```
webvpn# show web install status svc
SSLVPN Package SSL-VPN-Client version installed:
CISCO STC win2k+ 1.0.0
1,1,1
Tue 04/08/2005 15:31:20.43
```

This example shows how to display information about the files included in the SVC package:

```
webvpn# show web install package svc
SSLVPN Package SSL-VPN-Client installed:
File: \webvpn\stc\1\binaries\detectvm.class, size: 555
File: \webvpn\stc\1\binaries\java.htm, size: 309
File: \webvpn\stc\1\binaries\main.js, size: 8049
File: \webvpn\stc\1\binaries\ocx.htm, size: 244
File: \webvpn\stc\1\binaries\setup.cab, size: 164216
File: \webvpn\stc\1\binaries\stc.exe, size: 90104
File: \webvpn\stc\1\binaries\stcjava.cab, size: 6154
File: \webvpn\stc\1\binaries\stcjava.jar, size: 4053
File: \webvpn\stc\1\binaries\stcweb.cab, size: 12668
File: \webvpn\stc\1\binaries\update.txt, size: 9
File: \webvpn\stc\1\empty.html, size: 214
File: \webvpn\stc\1\images\alert.gif, size: 2042
File: \webvpn\stc\1\images\buttons.gif, size: 1842
File: \webvpn\stc\1\images\loading.gif, size: 313
```

```
File: \webvpn\stc\l\images\title.gif, size: 2739
File: \webvpn\stc\l\index.html, size: 4725
File: \webvpn\stc\l\index.html, size: 325
File: \webvpn\stc\version.txt, size: 63
Total files: 18
```

This example shows how to display the contents of a specific file:

```
webvpn# show web install file \webvpn\stc\version.txt
SSLVPN File \webvpn\stc\version.txt installed:
CISCO STC win2k+ 1.0.0
1,1,1
Tue 04/08/2005 15:31:20.43
webvpn#
```

show webvpn nbns

To display information on WebVPN NBNS cache, use the show webvpn nbns command.

show webvpn nbns context {name | all}

Syntax Description

name	Name of the context.
all	Displays information for all contexts.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module	Support for this command was introduced on the Catalyst 6500 series
Release 1.1	switches.

Examples

This example shows how to display status information about the NBNS cache for a specified context:

webvpn#

This example shows how to display status information about the NBNS cache for all contexts:

webvpn# NetBIOS		nbns context all IP Address	Timestamp
0 total NetBIOS	entries name	IP Address	Timestamp
0 total NetBIOS	entries name	IP Address	Timestamp
0 total NetBIOS	entries name	IP Address	Timestamp
0 total NetBIOS	entries name	IP Address	Timestamp
0 total webvpn#	entries		

show webvpn platform buffers

To display information about TCP buffer usage, use the show webvpn platform buffers command.

show webvpn-platform buffers [module module]

Syntax Description

module module	(Optional) Valid values for <i>module</i> are as follows:	
	all—all CPUs	
	fdu—FDU CPU	
	ssl1—SSL1 CPU	
	tcp1—TCP1 CPU	

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display the buffer usage and other information in the TCP subsystem:

```
webvpn# show webvpn-platform buffers module all
```

```
Buffers info for TCP module 1

TCP data buffers used 3340 limit 88064

TCP ingress buffer pool size 44032 egress buffer pool size 44032

TCP ingress data buffers min-thresh 5636096 max-thresh 9017344

TCP ingress data buffers used Current 0 Max 27

TCP ingress buffer RED shift 9 max drop prob 10

Conns consuming ingress data buffers 0

Buffers with App 0

TCP egress data buffers used Current 0 Max 115

Conns consuming egress data buffers 0

In-sequence queue bufs 0 000 bufs 0

Per-flow avg qlen 0 Global avg qlen 0

webvpn#
```

Related Commands

webvpn policy tcp

show webvpn platform context

To display information on WebVPN context, use the show webvpn platform context command.

show webvpn platform context name [module module]

Syntax Description

name	Name of the context.	
module module	Valid values for <i>module</i> are as follows:	
	all—all CPUs	
	fdu—FDU CPU	
	ssl1—SSL1 CPU	
	tcp1—TCP1 CPU	
	tcp2—TCP2 CPU	

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display status information about the specified context:

```
webvpn# show webvpn platform context tunnel
Certificate authentication type: peer certificate is always accepted
Admin Status: up
Operation Status: up
webvpn#
```

This example shows how to display all module status information about the specified context:

webvpn# show webvpn platform context tunnel module all

```
FDU Service Entry
                                              : 0
   Service ID : 8
                                 Protocol
   Virtual IP : 0.0.0.0 Virtual port : 0
   HTTP-redirect: 0
   Hash Index : 0
                                  Conn Count
                                              : 0
                : 0
                                              : DOWN
   Bound ID
                                  State
Service ID 8
 IP address : 116.117.110.110 Port : 0
 MSS : 1460
 SYN timeout (s): 75
 Idle timeout (s): 600
  FIN wait timeout (s): 75
  Reassembly timeout (s): 60
```

Connection Rx Buffer Size : 32768 Connection Tx Buffer Size : 65536

TOS Carryover Disabled

Service entry in cpu 1: Cipher suites: 0xF Versions: 0x3 Options: 0x6

Current Certificate Index: 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Certificate Index at 0 location: 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 Certificate Index at 1 location: 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Flags: 0x202

Handshake timeout: 0 secs Session timeout: 0 secs Session cache size: 262144

show webvpn platform crash-info

To collect information about the software-forced reset from the WebVPN Services Module, use the **show** webvpn platform crash-info command.

show webvpn platform crash-info [brief | details]

~ .		
Syntax	Descr	nottat

brief	(Optional) Collects a small subset of software-forced reset information, limited to processor registers.
details	(Optional) Collects the full set of software-forced reset information, including exception and interrupt stacks dump (this operation can take up to 10 minutes to complete printing).

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to collect a small subset of software-forced reset information:

webvpn# show webvpn platform crash-info brief

```
==== SSLVPN SERVICE MODULE - START OF CRASHINFO COLLECTION =====
----- COMPLEX 0 [VPN_IOS] -----
NVRAM CHKSUM: 0xDABB
NVRAM MAGIC: 0xC8A514F0
NVRAM VERSION: 1
HW_CID: 0
  APPLICATION VERSION: SVCWEBVPN Software (SVCWEBVPN-K9Y9-M), Version 12.3(7.11
)VA(0.117) INTERIM SOFTWARE \nCompiled Wed 13-Apr-05 02:20 by integ
  APPROXIMATE TIME WHEN CRASH HAPPENED: 02:56:38 UTC Sep 1 2005
  THIS CORE DIDN'T CRASH
  TRACEBACK: 374110 375C0C
  CPU CONTEXT -----
$0 : 00000000, AT : 01050000, v0 : 00000000, v1 : 01050000
a0 : 0104F3E0, a1 : 0208A390, a2 : 00000000, a3 : 00000000
t0 : 00000000, t1 : 032B8BC8, t2 : 00000001, t3 : FFFF00FF
t4 : 00368100, t5 : 74696F6E, t6 : 00000000, t7 : 39353438
s0 : 01050000, s1 : 01051F40, s2 : 028E16E0, s3 : 00BA0000
```

```
s4 : 00BA0000, s5 : 00BA0000, s6 : 01050000, s7 : 01050000
t8 : ODODODOD, t9 : 00000000, k0 : 00400001, k1 : 00000000
gp : 00FC65E0, sp : 028E16D0, s8 : 00000000, ra : 00374160
LO : F88923EA, HI : DA46BB94, BADVADDR : B60ED79D
EPC : 00374110, ErrorEPC : BFC00C70, SREG : 3400FD03
Cause 00004000 (Code 0x0): Interrupt exception
CACHE ERROR registers -----
CacheErrI: 00000000, CacheErrD: 00000000
ErrCtl: 00000000, CacheErrDPA: 000000000000000
HW CID: 1
  APPLICATION VERSION: SVCWEBVPN Software (SVCWEBVPN-K9Y9-M), Version 12.3(7.11
)VA(0.117) INTERIM SOFTWARE \nCompiled Wed 13-Apr-05 02:51 by integ
  APPROXIMATE TIME WHEN CRASH HAPPENED: 02:56:36 UTC Sep 1 2005
  THIS CORE CRASHED
  TRACEBACK: 1C6C7EC 1CC1B20 1CBEC14 1CBEDA8 1CC16EC 1CC1E7C 1CC96C4 1CC9930 1C
C94DC 1CCA570 1CBDF58 1CB69FC 1CB1898 1C7F964 1CE3618 1CE431C
$0 : 00000000, AT : 021D0000, v0 : 00000001, v1 : 00000000
a0 : OCFA6952, a1 : 00000000, a2 : 00000002, a3 : 00000062
t0 : 00000001, t1 : 00000000, t2 : 00000001, t3 : 00000062
t4 : 00000048, t5 : 0A0D0A0D, t6 : 0A0D0A0A, t7 : 090A0A0A
s0 : 00000000, s1 : 0CFA6950, s2 : 0D583008, s3 : 0CFA6950
s4 : OCFA6953, s5 : 02270000, s6 : 17394FC8, s7 : OD4708B8
t8 : 00000005, t9 : 00000001, k0 : 00000000, k1 : 00000000
gp : 021D4080, sp : 0CCE3840, s8 : FFFFFFFF, ra : 01CC1B20
LO : 00000003, HI : 0238A2C0, BADVADDR : 00000000
EPC : 01C6C7EC, ErrorEPC : 01572900, SREG : 3400FD03
Cause 000000C (Code 0x3): TLB (store) exception
CACHE ERROR registers -----
CacheErrI: 00000000, CacheErrD: 00000000
ErrCtl: 00000000, CacheErrDPA: 000000000000000
----- COMPLEX 1 [FDU_TCP_SSL_1] ------
NVRAM CHKSUM: 0x3C34
NVRAM MAGIC: 0xC8A514F0
NVRAM VERSION: 1
HW CID: 2
  APPLICATION VERSION: 2005.03.15 22:14:57 built for mahesh
  APPROXIMATE TIME WHEN CRASH HAPPENED: 11:28:14 UTC Aug 1 2005
  THIS CORE CRASHED
  TRACEBACK: 20A994 20B000 243C54 2444C8 24FF90 21A088 219970 2263B0 2523FC
  CPU CONTEXT -----
$0 : 00000000, AT : 00270000, v0 : 0000005C, v1 : 00285760
a0 : 12630E54, a1 : 00000000, a2 : 00000000, a3 : 00000000
t0 : 00000000, t1 : 34007E01, t2 : 34007100, t3 : FFFF00FF
t4 : 0020A9C0, t5 : 82602460, t6 : 00000002, t7 : 00000001
s0 : 12630E54, s1 : 002824DC, s2 : 12630C5C, s3 : 12630C5C
s4 : 002E0000, s5 : 00000003, s6 : 12630C20, s7 : 0026B258
t8 : FFFFFFF, t9 : 0160A2A0, k0 : 00400001, k1 : 00000000
gp : 00273320, sp : 09DFFD40, s8 : 12630C20, ra : 0020B000
```

```
LO : 00000000, HI : 0000004E, BADVADDR : 12630E54
EPC : 0020A994, ErrorEPC : F7EF23EA, SREG : 34007E03
Cause 00008014 (Code 0x5): Address Error (store) exception
CACHE ERROR registers -----
CacheErrI: 00000000, CacheErrD: 00000000
ErrCtl: 00000000, CacheErrDPA: 000000000000000
HW_CID: 3
  APPLICATION VERSION: 2005.03.15 22:14:57 built for mahesh
  APPROXIMATE TIME WHEN CRASH HAPPENED: 11:28:14 UTC Aug 1 2005
  THIS CORE DIDN'T CRASH
  TRACEBACK: 449F70 433458 42D0A0 422694
  CPU CONTEXT -----
$0 : 00000000, AT : 00490000, v0 : 00000000, v1 : 0E1743D8
a0 : 09E0A534, a1 : 00000002, a2 : 00000002, a3 : 00000002
t0 : 00006100, t1 : 00000000, t2 : B0060100, t3 : FFFF00FF
t4 : 0040A9C0, t5 : A295B1CD, t6 : B22AEDDB, t7 : F9D0B2AC
s0 : 09E0A4E8, s1 : 0048F698, s2 : 00000000, s3 : 0048F600
s4 : 00000000, s5 : 00000000, s6 : 00480000, s7 : 00480000
t8 : 00000002, t9 : 00000001, k0 : 00000000, k1 : 00000000
gp : 004965E0, sp : 123FFF30, s8 : 00000001, ra : 00433458
LO : 999999C9, HI : 0000001F, BADVADDR : 644E427A
EPC : 00449F70, ErrorEPC : FFDF6777, SREG : 34007E03
Cause 0000C000 (Code 0x0): Interrupt exception
CACHE ERROR registers -----
CacheErrI: 00000000, CacheErrD: 00000000
ErrCtl: 00000000, CacheErrDPA: 000000000000000
==== SSLVPN SERVICE MODULE - END OF CRASHINFO COLLECTION ======
```

show webvpn platform gateway

To display gateway information WebVPN, use the show webvpn platform gateway command.

show webvpn platform gateway name [debug | module module]

Syntax Description

name	Name of the gateway.
debug	(Optional) Displays debug information for the gateway.
module module (Optional) Valid values for module are as follows:	
	all —all CPUs
	fdu—FDU CPU
	ssl1—SSL1 CPU
	tcp1—TCP1 CPU
	tcp2—TCP2 CPU

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display status information for a specific gateway:

```
webvpn# show webvpn platform gateway tunnel
IP: 10.1.2.14, port: 443
rsa-general-purpose certificate trustpoint: mytp
Certificate chain for new connections:
    Certificate:
        Key Label: mytp, 1024-bit, not exportable
        Key Timestamp: 12:09:27 UTC Dec 25 2004
        Serial Number: 0FE5
    Root CA Certificate:
        Serial Number: 01
Certificate chain complete
Admin Status: up
Operation Status: up
webvpn#
```

This example shows how to display debug information for a specific gateway:

```
webvpn# show webvpn platform gateway s1 debug
IP: 10.1.2.14, port: 443
rsa-general-purpose certificate trustpoint: mytp
 Certificate chain for new connections:
   Certificate:
      Key Label: mytp, 1024-bit, not exportable
      Key Timestamp: 12:09:27 UTC Dec 25 2004
      Serial Number: 0FE5
   Root CA Certificate:
      Serial Number: 01
 Certificate chain complete
Admin Status: up
Operation Status: up
Service ID: 1
                   Bound ID: -1
Virtual IP: 10.1.2.14
                               Port
VLAN ID : 0
                     MAC Address: 0000.0000.0000
State
        : PROXY VALID
Enabled : Yes
Secondary : No
Client NAT: disable
Server NAT: disable
webvpn#
```

This example shows how to display status information for all CPUs for a specific gateway:

```
webvpn# show web platform gateway s1 module all
```

```
FDU Service Entry
   Service ID : 1
                                  Protocol
   Virtual IP : 64.102.223.140
                                  Virtual port : 443
   HTTP-redirect: 0
   Hash Index : 896
                                               : 0
                                  Conn Count
   Bound ID
              : -1
                                  State
Service ID 1
  IP address : 10.1.2.14 Port : 443
 MSS : 1460
  SYN timeout (s): 75
  Idle timeout (s): 600
  FIN wait timeout (s): 75
 Reassembly timeout (s): 60
  Connection Rx Buffer Size : 32768
  Connection Tx Buffer Size : 65536
  TOS Carryover Disabled
Service entry in cpu 1:
   Cipher suites: 0xF
   Versions: 0x3
    Options: 0x6
    Current Certificate Index: 0x0 0x1 0x0 0x0 0x0 0x0 0x0
    Certificate Index at 0 location: 0x0 0x0 0x0 0x0 0x0 0x0 0x0
    Certificate Index at 1 location: 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
   Flags: 0x201
    Handshake timeout: 0 secs
    Session timeout: 0 secs
    Session cache size: 262144
```

show webvpn platform mac address

To display the current MAC address, use the show webvpn platform mac address command.

show webvpn platform mac address

Syntax Description This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes EXEC

Command History

Release	Modification
WebVPN Module	Support for this command was introduced on the Catalyst 6500 series
Release 1.1	switches.

Examples

This example shows how to display the current MAC address that is used in the WebVPN Services Module:

webvpn# show webvpn platform mac address SVCWEBVPN module MAC address: 000d.29f0.c24c

show webvpn platform policy

To display the SSL or TCP policy information, use the show webvpn platform policy command.

show webvpn platform policy {ssl | tcp} name

S١	/ntax	Description

ssl	Specifies the SSL policy.
tcp	Specifies the TCP policy.
name	Name of the SSL or TCP policy.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display SSL policy information on the WebVPN Services Module:

webvpn# show webvpn platform policy ssl

SSL Policy Name

Usage-Count

show webvpn platform version

To display the current image version, use the show webvpn platform version command.

show webvpn platform version

Syntax Description This command has

This command has no arguments or keywords.

Defaults This command has no default settings.

Command Modes EXEC

Command History

Release	Modification
WebVPN Module	Support for this command was introduced on the Catalyst 6500 series
Release 1.1	switches.

Examples

This example shows how to display the image version that is currently running on the WebVPN Services Module:

webvpn# show webvpn platform version

Cisco IOS Software, SVCWEBVPN Software (SVCWEBVPN-K9Y9-M), Version 12.3(8)VA(1.1) Copyright (c) 1986-2005 by Cisco Systems, Inc. Compiled Thu 26-May-05 02:44 by integ

ROM: System Bootstrap, Version 12.2(11)YS1 RELEASE SOFTWARE

webvpn-alpha uptime is 5 days, 19 hours, 51 minutes System returned to ROM by power-on System image file is "tftp://10.1.1.1/unknown" AP Version 1.1(0.97)

show webvpn platform vlan

To display VLAN information, use the show webvpn platform vlan command.

show webvpn platform vlan [vlan-id]

Syntax	

vlan-id	(Optional) VLAN ID. Displays information for a specific VLAN; valid
	values are from 2 to 1005.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Services Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display all the VLANs that are configured on the WebVPN Services Module:

webvpn# show webvpn platform vlan Vlan-id IP address NetMask VRF ---- ----- ---- 10 10.81.12.3 255.255.255.0

20.102.223.139 255.255.255.248

This example shows how to display information about a specific VLAN on the WebVPN Services Module:

$\verb|webvpn#| \textbf{show webvpn platform vlan 10}|\\$

Vlan-id	IP address	3	NetMask	VRF
		-		
10	10.81.12.3	3	255.255.255.0	_
FI	OU module i	in	fo	
FDU Vlan	Entry			
VLAN	ID	:	10	
My II	P Addr	:	10.81.12.3	
My Ne	et Mask	:	255.255.255.0	
VRF I	ID	:	0	

show webvpn policy

To display the configured WebVPN policies, use the show webvpn policy command.

show webvpn policy {**group** name **context** name | **tcp** [name] | **ssl** [name]}

Syntax Description

group name context name	Displays the group policies for the specified context.
tcp	Displays the configured TCP policies.
ssl	Displays the configured SSL policies.
name	(Optional) Policy name.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Examples

This example shows how to display information about the HTTP header policy:

```
webvpn# show web policy group tunnel context tunnel
WEBVPN: group policy = tunnel ; context = tunnel
   idle timeout = 2100 sec
   session timeout = 43200 sec
   functions = svc-enabled
   address pool name = "addr"
   dpd client timeout = 300 sec
   dpd gateway timeout = 300 sec
   keep sslvpn client installed = disabled
   rekey interval = 3600 sec
   rekey method = ssl
   lease duration = 43200 sec
webvpn#
```

Related Commands

webvpn policy ssl webvpn policy tcp

show webvpn session

To display information about the WebVPN session, use the show webvpn session command.

show webvpn session {context {name | all} | user name context {name | all}}

Syntax Description

context name	Specifies the context name.
user name	Specifies the user name.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Module	Support for this command was introduced on the Catalyst 6500 series
Release 1.1	switches.

Examples

This example shows how to display session information about the specified context:

```
webvpn# show webvpn session context c1
```

WebVPN context name: c1

 Client_Login_Name
 Client_IP_Address
 No_of_Connections
 Created
 Last_Used

 user1
 10.2.1.220
 2
 04:47:16
 00:01:26

 user2
 10.2.1.221
 2
 04:48:36
 00:01:56

This example shows how to display session information for a specific user:

webvpn# show webvpn session user user1 context c1

```
WebVPN user name = user1 ; IP address = 10.2.1.220 ; context = c1
    No of connections: 2
    Created 04:50:21, Last-used 00:00:31
    Client Port: 2503, Server IP Addr: 10.102.31.9, Server Port: 80
    Client Port: 2504
    User Policy Parameters
      Group name = test
    Group Policy Parameters
      url list name = "Cisco test URL list"
      idle timeout = 2100 sec
      session timeout = 43200 sec
      port forward name = "Mail Servers"
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep sslvpn client installed = disabled
      rekey interval = 3600 \text{ sec}
      rekey method = ssl
      lease duration = 43200 sec
```

show webvpn stats

To display information about the statistics counter, use the **show webvpn stats** command.

show webvpn stats [type]

Syntax Description

type (Optional) See the "Usage Guidelines" section for additional informa

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
WebVPN Services Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The valid options for *type* are as follows:

- cifs [detail][context {name | all}]
- context {name | all}
- detail [context {name | all}]
- mangle [detail][context {name | all}]
- port-forward [detail][context {name | all}]
- socket [detail][context {name | all}]
- tunnel [detail][context {name | all}]

Examples

This example shows how to display all the statistics counters that are collected on the WebVPN Services Module:

webvpn# show webvpn stats

```
User session statistics:
                                       AAA pending reqs
   Active user sessions
   Peak user sessions
                          : 6
                                        Peak time
                                                               : 17:22:16
                           : 2
                                       Terminated user sessions : 29
   Active user TCP conns
   Session alloc failures : 0
                                       Authentication failures : 3
   VPN session timeout
                           : 1
                                       VPN idle timeout
   User cleared VPN sessions: 0
                                       Exceeded ctx user limit : 0
    Exceeded total user limit: 0
```

Mangling statistics:			
	15705	Absolute urls	41850
Non-http(s) absolute urls:	9306	Non-standard path urls	: 1005
Interesting tags :	200329	Uninteresting tags	398899
Interesting attributes :	164642	Uninteresting attributes	272669
Embedded script statement:	10226	Embedded style statement	2800
Inline scripts :	34868	Inline styles	26475
HTML comments :	6018	HTTP/1.0 requests	148
HTTP/1.1 requests :	8115	Unknown HTTP version	: 0
GET requests :	6290	POST requests	95
CONNECT requests :	0	Other request methods	: 1878
Through requests :	6172	Gateway requests	2091
Pipelined requests :	7	Req with header size >1K	: 1
Processed req hdr bytes :	5320280	Processed req body bytes	529871
HTTP/1.0 responses :	797	HTTP/1.1 responses	6277
HTML responses :	1919	CSS responses	80
XML responses :	2476		: 171
Other content type resp :	1435	Chunked encoding resp	: 1926
Resp with encoded content:	0	Resp with content length	3926
Close after response :	1222	Resp with header size >1K	: 0
Processed resp hdr size :	1870948	Processed resp body bytes	65670616
-	245	Chunked encoding requests	
CIFS statistics:			
SMB related Per Context:			
TCP VC's :	0	UDP VC's	: 0
Active VC's :	0	Active Contexts	: 0
Aborted Conns :	0		
NetBIOS related Per Context:			
Name Queries :	0	Name Replies	: 0
NB DGM Requests :	0	NB DGM Replies	: 0
NB TCP Connect Fails :	0	NB Name Resolution Fails	: 0
SMB related Global:			
Sessions in use :	0	Mbufs in use	: 0
Mbuf Chains in use :	0	Active VC's	: 0
Active Contexts :	0	Browse Errors	: 0
Empty Browser List :	0	NetServEnum Errors	: 0
Empty Server List :	0	NBNS Config Errors	: 0
NetShareEnum Errors :	0		
HTTP related Per Context:			
Requests :	24	Request Bytes RX	8508
Request Packets RX :	0	Response Bytes TX	1465966
Response Packets TX :	975	Active Connections	: 0
Active CIFS context :	0	Requests Dropped	: 0
HTTP related Global:			
Server User data :	0	CIFS User data	: 0
Net Handles :	0	Active CIFS context	: 0
Authentication Fails :	0	Operations Aborted	: 0
Timers Expired :	0	Pending Close	: 0
Net Handles Pending SMB :	0	File Open Fails	: 0
Browse Network Ops :	0	Browse Network Fails	: 0
Browse Domain Ops :	0	Browse Domain Fails	: 0
	0	Browse Server Fails	: 0
	0	Browse Share Fails	: 0
-	0	Browse Network Fails	: 0
-	0	File Read Fails	: 0
<u>-</u>	0	File Write Fails	: 0
-	0	Folder Create Fails	: 0
_	0		: 0
_	0		: 0
-			

Socket statistics:					
Sockets in use	:	2	Sock Usr Blocks in use	:	2
Sock Data Buffers in use	:	0	Sock Buf desc in use	:	0
Select timers in use	:	2	Sock Select Timeouts	:	0
Sock Tx Blocked	:	49	Sock Tx Unblocked	:	49
Sock Rx Blocked	:	0	Sock Rx Unblocked	:	0
Sock UDP Connects	:	0	Sock UDP Disconnects	:	0
Sock Premature Close	:	0	Sock Pipe Errors	:	5
Port Forward statistics:					
Client			Server		
in pkts	:	0	out pkts	:	0
in bytes	:	0	out bytes	:	0
out pkts	:	0	in pkts	:	0
out bytes	:	0	in bytes	:	0
Tunnel Statistics:					
Active connections	:	0			
Peak connections	:	1	Peak time	:	5d16h
Connect succeed	:	6	Connect failed	:	0
Reconnect succeed	:	1	Reconnect failed	:	0
DPD timeout	:	0			
Client			Server		
in CSTP frames	:	23098	out IP pkts	:	23093
in CSTP data	:	23093			
in CSTP control	:	5			
in CSTP bytes	:	4956832	out IP bytes	:	4771852
out CSTP frames	:	32086	in IP pkts	:	32084
out CSTP data	:	32084			
out CSTP control	:	2			
out CSTP bytes	:	16136526	in IP bytes	:	16512477

webvpn#

Most of the counters are self-explanatory. The following descriptions are for the counters that are not self-explanatory:

- User session statistics:
 - Terminated user sessions—Number of sessions that were logged out from the time last clear keyword was executed.
 - Session alloc failures—Indicates that the system is running out of memory.
 - Authentication failures—AAA responded with failure status for given username or password .
 - VPN session timeout—Number of sessions that were cleared because of session timeout expiry.
 - VPN idle timeout—Number of sessions that were cleared because of idle timeout expiry.
 - User cleared vpn sessions—Number of sessions that were cleared because of the clear webvpn session command.
 - Exceeded ctx user limit—Number of sessions that were rejected because of exceeding max-users limit configured under context.
 - Exceeded total user limit—Number of sessions that were rejected because of exceeding the system user limit (currently 8000).

Mangling statistics:

- Close after response—Number of connections that were closed after sending responses because of lack of content length.

CIFS statistics:

- SMB-related counters per context:

TCP/UDP VC's—Back-end TCP/UDP connections established successfully so far.

Active VC's—Currently active TCP/UDP connections.

Active Contexts—Currently active SMB contexts.

Aborted Conns—TCP connections aborted by the peer.

- NetBIOS-related counters per context:

Name Queries—NBNS name queries sent.

Name Query Replies—NBNS name query replies received. Mismatch indicates that browsers, PDC, and servers could not be contacted.

NBDGM requests—NB datagram service-related get backup browser list queries sent.

NBDGM replies—NB datagram service-related get backup browser list replies received. Request and reply mismatch indicates that browse domain attempt would not work.

NB TCP connect fails—NB TCP connection attempts that resulted in failures. Indicates connectivity issues to PDC and file servers.

- SMB-related counters for all contexts:

Sessions in Use—Back-end SMB sessions in use (active)

Mbufs in use—Application buffer descriptors in use.

Mbuf Chains in use—Application buffers in use.

Active VCs—Total active back-end SMB connections in the system.

Active Context—Total active back-end SMB context in the system.

Browse Errors—Indicates failed browse domain attempts.

Empty Browse list—Indicates number of times empty backup browse list replies received.

NetServEnum errors—Indicates number of failed attempts at receiving list of servers in a specific domain.

NetShareEnum errors—Indicates number of failed attempts at receiving list of files and folders in a specific share.

HTTP-related counters per context:

Active Connections—Connections on which CIFS requests are being processed.

Active CIFS Context—CIFS application module context on which CIFS requests are being processed.

- HTTP-related counters for all contexts:

Server User Data—Number of entries in the per server username and password cache.

CIFS User Data—Default username and password cache entries.

Net Handles—Total connections in the system (includes active as well as idle).

Active CIFS context—Global count of active CIFS application module contexts.

Authentication fails—CIFS HTTP requests processed without a WebVPN cookie or an expired WebVPN cookie.

Operations Aborted—Back-end operations that were aborted because the HTTP connection was lost. Indicates that CIFS transactions are not completing successfully.

Pending Close—Number of times close is pending, waiting for Tx to unblock and finish sending pending data.

· Socket statistics:

- Tx Blocked—Number of times that application send was blocked by TCP congestion control.
- Tx Unblocked—Number of times that application send resumed after being blocked due to TCP congestion control. If transmit blocked and unblocked do not match after a sufficient period of time, then the transaction is stalled.
- Rx Blocked—Number of times application blocked further reception of data from TCP layer.
 This indicates application buffer starvation or processing limit.
- Rx Unblocked—Number of times application resumed further reception of data from TCP layer.
 If receive blocked and unblocked do not match after a sufficient period of time, then the transaction is stalled.
- Premature Close—Number of times that application closed the connection before it could be established.
- Select Timeouts—Number of times that application timed out while waiting for a reply in a request and reply exchange or waiting for a TCP connection to be established.

This example shows how to display CIFS statistics on the WebVPN Services Module:

webvpn# show webvpn stats cifs CIFS statistics: SMB related Per Context: TCP VC's : 0 UDP VC's : 0 Active VC's : 0 Aborted Conns : 0 Active Contexts : 0 NetBIOS related Per Context: Name Queries : 0 Name Replies : 0 NB DGM Requests : 0 NB DGM Replies : 0 NB TCP Connect Fails : 0 NB Name Resolution Fails : 0 Sessions in use : 0 Mbufs in use Mbuf Chains in use : 0 Active VC's Active Contexts : 0 Browse Errors Empty Browser List : 0 NetServEnum Errors Empty Server List : 0 NBNS Config Errors NetShareEnum Errors : 0 TTP related Per Contexts SMB related Global: : 0 : 0 : 0 HTTP related Per Context: : 24 : 8508 Requests Request Bytes RX Response Bytes TX Request Packets RX : 0 : 1465966 Response Packets TX : 975 Active CIFS context : 0 Active Connections : 0 Requests Dropped : 0 HTTP related Global: TTP related Global: Server User data : 0 CIFS User data Net Handles : 0 Active CIFS context Authentication Fails : 0 Operations Aborted Timers Expired : 0 Pending Close Net Handles Pending SMB : 0 File Open Fails Browse Network Ops : 0 Browse Network Fails Browse Domain Ops : 0 Browse Domain Fails Browse Server Ops : 0 Browse Server Fails Browse Share Ops : 0 Browse Share Fails Browse Dir Ops : 0 Browse Network Fails : 0 : 0 : 0 : 0 : 0 : 0 : 0

```
File Read Ops : 0 File Read Fails : 0
File Write Ops : 0 File Write Fails : 0
Folder Create Ops : 0 Folder Create Fails : 0
File Delete Ops : 0 File Delete Fails : 0
File Rename Ops : 0 File Rename Fails : 0
```

webvpn#

This example shows how to display the statistics for a specific context:

```
webvpn# show web stats context tunnel
WebVPN context name : tunnel
User session statistics:
      Active user sessions
                                                : 0
                                                                      AAA pending reqs
                                            .
: 1
      Peak user sessions
                                                                      Peak time
                                                                                                                  : 5d16h
      Active user TCP conns : 0
Session alloc failures : 0
VPN session timeout : 1
User cleared VPN sessions: 0
                                                                    Terminated user sessions : 5
                                                               Terminated user sessions
Authentication failures : 0
VPN idle timeout : 0
                                                                   Exceeded ctx user limit : 0
     gling statistics:

Relative urls : 0 Absolute urls : 0

Non-http(s) absolute urls: 0 Non-standard path urls : 0

Interesting tags : 0 Uninteresting tags : 0

Interesting attributes : 0 Uninteresting attributes : 0

Embedded script statement: 0 Embedded style statement : 0

Inline scripts : 0 Inline styles : 0

HTML comments : 0 HTTP/1.0 requests : 0

HTTP/1.1 requests : 111 Unknown HTTP version : 0

GET requests : 106 POST requests : 5

CONNECT requests : 0 Other request methods : 0

Through requests : 0 Gateway requests : 11

Pipelined requests : 0 Req with header size >1K : 0

Processed req hdr bytes : 43741 Processed req body bytes : 26
Mangling statistics:
Relative urls : 0
                                                                                                                  : 111
      Pipelined requests . u

Processed req hdr bytes : 43741 Processed req body bytes . 20

: 0 HTTP/1.1 responses : 0

: 0
     Processed req hdr bytes : 43741
HTTP/1.0 responses : 0
HTML responses : 0

XML responses : 0
Other content type resp : 0
Resp with encoded content: 0
Close after response : 0
Processed resp hdr size : 0
Backend https response : 0

Chunked encoding resp : 0
Resp with header size >1K: 0
Processed resp bdy bytes: 0
Backend https response : 0

Chunked encoding requests: 0
                                                                      Processed req body bytes: 265
CIFS statistics:
   SMB related Per Context:
      TCP VC's
Active VC's
                                              : 0
                                                                      UDP VC's
                                              : 0
                                                                       Active Contexts
                                                                                                                  : 0
      Aborted Conns : 0
   NetBIOS related Per Context:
      Name Queries : 0
                                                                      Name Replies
                                                                                                                  : 0
      NB DGM Requests
                                                                       NB DGM Replies
      NB TCP Connect Fails : 0
                                                                       NB Name Resolution Fails : 0
   HTTP related Per Context:
                                              : 5
                                                                                                                : 1840
                                                                      Request Bytes RX
      Requests
                                              : 0
      Request Packets RX
                                                                      Response Bytes TX
                                                                                                               : 1435222
      Response Packets TX : 938
Active CIFS context : 0
                                                                       Active Connections
                                                                                                               : 0
                                                                       Requests Dropped
                                                                                                                  : 0
Socket statistics:
                                                                Sock Usr Blocks in use
       Sockets in use : 0
                                                                      Sock Buf desc in use
       Sock Data Buffers in use : 0
                                                                                                                  : 0
      Select timers ...

Sock Tx Blocked : 0

Thocked : 0
                                                                      Sock Select Timeouts
                                                                                                                  : 0
                                                                                                               : 0
                                                                      Sock Tx Unblocked
                                                                       Sock Rx Unblocked
                                                                                                                  : 0
```

Sock UDP Connects	: 0	Sock UDP Disconnects	: 0
Sock Premature Close	: 0	Sock Pipe Errors	: 0
Port Forward statistics:			
Client		Server	
in pkts	: 0	out pkts	: 0
in bytes	: 0	out bytes	: 0
out pkts	: 0	in pkts	: 0
out bytes	: 0	in bytes	: 0
Tunnel Statistics:			
Active connections	: 0		
Peak connections	: 1	Peak time	: 5d16h
Connect succeed	: 6	Connect failed	: 0
Reconnect succeed	: 1	Reconnect failed	: 0
DPD timeout	: 0		
Client		Server	
in CSTP frames	: 23098	out IP pkts	: 23093
in CSTP data	: 23093		
in CSTP control	: 5		
in CSTP bytes	: 4956832	out IP bytes	: 4771852
out CSTP frames	: 32086	in IP pkts	: 32084
out CSTP data	: 32084		
out CSTP control	: 2		
out CSTP bytes	: 16136526	in IP bytes	: 16512477

snmp-server enable

To configure the SNMP traps and informs, use the **snmp-server enable** command. Use the **no** form of this command to disable SNMP traps and informs.

[no] snmp-server enable {informs | traps {ipsec | isakmp | snmp | tty}}

Syntax Description

informs	Enables SNMP informs.
traps	Enables SNMP traps.
ipsec	Enables IPSec traps. See the "Usage Guidelines" section for additional options.
isakmp	Enables ISAKMP traps. See the "Usage Guidelines" section for additional options.
snmp	Enables SNMP traps. See the "Usage Guidelines" section for additional options.
tty	Enables TCP connection traps.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
SSL Services Module	Support for this command was introduced on the Catalyst 6500 series
Release 2.1(1)	switches.

Usage Guidelines

The **ipsec** keyword has the following options:

- ipsec crptomap {add | attach | delete | detach}
- ipsec too-many-sas
- ipsec tunnel {start | stop}

The **isakmp** keyword has the following options:

• isakmp {policy {add | delete} | tunnel {start | stop}}

The **snmp** keyword has the following options:

 $\bullet \quad snmp \ [authentication \ | \ coldstart \ | \ linkdown \ | \ linkup \ | \ warmstart]$

Examples

This example shows how to enable SNMP informs:

```
wwbvpn(config)# snmp-server enable informs
wwbvpn(config)#
```

This example shows how to enable traps:

```
wwbvpn(config)# snmp-server enable traps
wwbvpn(config)#
```

This example shows how to enable authentication traps:

```
\label{lem:wwbvpn} wwbvpn(\texttt{config}) \# \ \textbf{snmp-server} \ \textbf{enable} \ \textbf{traps} \ \textbf{snmp} \ \textbf{authnetication} \\ wwbvpn(\texttt{config}) \# \\
```

SVC

To configure the tunnel capabilities for a group-policy context, use the **svc** command. Use the **no** form of this command to remove any of the **svc** commands that you have entered.

svc command

Syntax Description	command	Specifies the configuration command; see Table 2-5 for a list of available commands.
-		

Defaults See Table 2-5 for the default settings.

Command Modes WebVPN group context submode

Command History	Release	Modification
	WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines The prompt for the svc command is the same as the group-policy prompt.

Table 2-5 lists the commands available to configure tunnel-mode capability for a group context.

Table 2-5 Tunnel-Mode Configuration Commands

Command	Purpose and Guidelines	Default
address-pool address-pool-name	Assigns addresses from the pool to the remote users.	
default-domain default-domain-name	Specifies the default domain to be used for the user/group, if tunnel-mode WebVPN is enabled for the user/group.	
dns-server (primary secondary) ip-address	Specifies the primary and secondary DNS servers for web browsing. After the SSL VPN client (SVC) is installed, the active web browser is deactivated and a new browser is launched. The DNS server information specified here is for the newly launched browser. Once the connection is closed, the previous DNS settings are reapplied.	

Table 2-5 Tunnel-Mode Configuration Commands (continued)

Command	Purpose and Guidelines	Default
<pre>dpd-interval {client timeout} {gateway timeout}</pre>	Specifies the dead peer detection (DPD) timeout values for the gateway or the client, if tunnel-mode WebVPN is enabled for the user or group. The DPD timer is used to determine if a DPD packet needs to be sent to the peer. The DPD timer is reset every time a Cisco SSL Tunnel Protocol (CSTP) frame is received from the peer.	Disabled for the gateway and the client.
	gateway timeout—Specifies the DPD timeout values for the SG; valid values are from 0 (disabled) to 3600 seconds.	
	client <i>timeout</i> —Specifies the DPD timeout values for the client; valid values are from 0 (disabled) to 3600 seconds.	
homepage url	Configures the URL of the web page to be displayed to the user upon login. The URL string specifies the path of the URL. The maximum length for the URL string is 255 characters. Entering the no form of this command removes the command from the configuration.	No web page is specified.
keep-client-installed	Keeps the SVC installed after the connection is closed.	
msie-proxy exception {ip-address dns-name}	Specifies the Microsoft Internet Explorer (MSIE) browser proxy settings.	Disabled.
	Note This command is supported only with the MSIE browser.	
	The exception keyword specifies a single DNS name or IP address for traffic that is not sent through a proxy.	
<pre>msie-proxy server {ip-address dns_name}[: port]</pre>	Specifies the Microsoft Internet Explorer (MSIE) browser proxy settings.	Disabled.
	Note This command is supported only with the MSIE browser.	
	The server keyword specifies an IP address or DNS name, optionally followed by a colon and port number, that is used by all the proxy settings in the browser (HTTP, Secure, FTP, Gopher) except Socks.	
msie-proxy option {auto bypass-local none}	Specifies the Microsoft Internet Explorer (MSIE) browser proxy settings.	option none
	Note This command is supported only with the MSIE browser.	
	The option none keyword specifies that the browser does not use a proxy.	
	The option auto keyword specifies that the browser proxy settings are automatically detected.	
	The option bypass-local keyword specifies that the local addresses bypass the proxy.	

Table 2-5 Tunnel-Mode Configuration Commands (continued)

Command	Purpose and Guidelines	Default
rekey method {new-tunnel ssl} no rekey method	Specifies the rekey method. Entering the no form of this command disables rekeying.	If rekeying is enabled, the default
	• new-tunnel —Terminates the existing tunnel and requests a new tunnel.	method is ssl .
	• ssl—Initiates an SSL rehandshake.	
rekey {time interval}	Specifies when the VPN client rekeys the SSL tunnel. This	21600 seconds
no rekey time	interval is time-based. Entering the no form of this command disables the rekey-time interval.	(6 hours).
	interval—Valid values are from 0 to 43200 seconds.	
split dns string	Specifies the split-tunnel parameters.	
	string—Name or IP address of the DNS server.	
split exclude {ip-address netmask local-lans}	Allows you to specify the traffic that is sent directly to an external website without being tunneled through the internal network; all other traffic is tunneled.	
	Note You can specify either the split include or the split exclude command; you cannot specify both keywords. You can specify up to 200 addresses for either the split include or split exclude keyword by entering the command multiple times.	
	• <i>ip-address netmask</i> —Address of traffic that is not tunneled.	
	• local-lans—Specifies that the end user's local LAN traffic is not tunneled.	
split include ip-address netmask	Allows you to specify the traffic that is tunneled; all other traffic is not tunneled through the internal network.	
	Note You can specify either the split include or the split exclude command; you cannot specify both keywords. You can specify up to 200 addresses for either the split include or split exclude keyword by entering the command multiple times.	
	ip-address netmask—Address of traffic that is tunneled.	
wins-server {primary secondary} ip-address	Specifies the primary or secondary WINS server.	

url-list

To enter the URL submode to configure the URL lists, use the **url-list** command. Use the **no** form of this command to remove the given list from the configuration.

url-list listname

no url-list listname

Syntax Description	listname	Name for the URL list.
Defaults	This command has no	default settings.
Command Modes	WebVPN context sub	mode
Command History	Release	Modification
	WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The *listname* argument is case-sensitive and can be a maximum of 64 characters.

After you enter the **url-list** command, the prompt changes to the following:

webvpn(config-webvpn-url)#

After you enter the URL submode, there are commands available to configure the URL lists. Table 2-6 lists the URL submode commands.

Table 2-6 URL Submode Commands

Command	Purpose and Guidelines	Default
exit	Exits WebVPN URL submode and returns to WebVPN context submode.	
heading text	Specifies the heading text for the group of URLs. Enclose the <i>text</i> value within quotation marks if the heading includes any spaces.	
	You can specify only one heading per list name.	
url-text text url-value url[/exchage]	Specifies the text the user sees for the link on their home page; the <i>text</i> must be unique within a given listname. Enclose the <i>text</i> value within quotation marks if the text includes any spaces.	

The **url-value** *url* keyword and argument specifies the URL that the link goes to. To use Outlook Web Access (OWA) for web-based email, append the URL with the **/exchange** keyword (requires authentication to an Exchange server).

You can specify multiple URLs for a given list name.

This example shows how to configure the URL list:

```
webvpn(config-webvpn-context)# url-list cisco
webvpn(config-webvpn-url)# url-text cisco url-value http://cisco.com
webvpn(config-webvpn-url)# url-text CNN url-value http://cnn.com
webvpn(config-webvpn-url)# url-text yahoo url-value http://yahoo.com
webvpn(config-webvpn-url)# url-text payroll url-value http://10.1.2.215/payroll
webvpn(config-webvpn-url)# url-text finance url-value https://finance.cisco.com
webvpn(config-webvpn-url)# url-text "OWA server" url-value http://mail.cisco.com/exchange
webvpn(config-webvpn-url)# exit
webvpn(config-webvpn-context)#
```

Related Commands

webvpn context

webvpn context

To enter the WebVPN context submode and define the virtual WebVPN context, use the **webvpn context** command. Use the **no** form of this command to remove any commands that you have entered in the WebVPN subcommand mode from the configuration.

webvpn context [vpn-name]

no webvpn context vpn-name

Syntax Description	vpn-name	(Optional) Name of the WebVPN instance.
Defaults	This command has no	default settings.
Command Modes	Global configuration	
Command History	Release	Modification
	WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The *vpn-name* argument is case-sensitive.

After you enter the webvpn context command, the prompt changes to the following:

webvpn(config-webvpn-context)#

After you enter the context submode, there are commands available to configure the context services. Table 2-7 lists the virtual context submode commands.

Table 2-7 Virtual WebVPN Context Submode Commands

Command	Purpose and Guidelines	Defaults
<pre>aaa authentication {{domain domain-list} {list listname}}</pre>	Specifies AAA configuration parameters for context. • domain domain-list—Specifies the name of the domain used for authentication.	
	• list <i>listname</i> —Specifies the name of the authentication list.	
default-group-policy default-policy-name	Specifies the default group policy that the virtual WebVPN context instance uses. See the policy group command for information on group policies.	
exit	Exits from the context submode and returns to the global configuration mode.	

Table 2-7 Virtual WebVPN Context Submode Commands

Command	Purpose and Guidelines	Defaults
<pre>gateway gateway-name {{domain-name domain-name} {virtual-host hostname}}</pre>	Specifies the corresponding virtual gateway instance configured on the secure gateway and the mapping methods (for example, IP address, URL, and domain name) as follows:	Virtualization is performed through a unique IP address.
	• gateway-name—Name of the virtual gateway configured on the system.	
	• domain-name <i>domain-name</i> —(Optional) Maps to a specific domain name. The <i>domain-name</i> argument is a ASCII string, which is used to specify a corporate-specific domain name (for example, cisco.com) for the virtual WebVPN instance.	
	• virtual-host <i>hostname</i> —(Optional) Maps to a specific virtual host.	
inservice	Brings context to inservice.	
login-message string no login-message	Specifies the text that prompts the user to login. Limited to 255 characters. Use the no form of this command to return to the default setting.	string is Please enter your username and password.
logo [file filename none]	Specifies the custom logo image that is displayed on the login and home pages.	
	file <i>filename</i> —(Optional) Specifies the filename of a file that is uploaded by the administrator to the security gateway.	
nat-address start-address end-address {netmask netmask}	Specifies the NAT addresses to be used in opening a server connection. The addresses specified in the nat-address command must match one of the subnets configured on the WebVPN subinterfaces.	
	• <i>start-address</i> —Starting IP address that defines the range of addresses in the address pool.	
	 end-address—Ending IP address that defines the range of addresses in the address pool. 	
	 netmask netmask—Network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong. 	
nbns-list name	Enters nbmslist submode and allows you to create the NBNS list name. See the nbns-list command for information on configuring the NBNS list.	
password-prompt prompt	Configures the initial WebVPN login password prompt. The maximum length of prompt is 16 characters.	prompt is Password:

Table 2-7 Virtual WebVPN Context Submode Commands

Command	Purpose and Guidelines	Defaults
policy group policy-name	Enters the group submode and allows you to configure group policy settings. See the policy group command for information on configuring the group policy.	
policy ssl policy-name	Specifies the SSL policy that the SSL protocol uses.	
policy tcp policy-name	Specifies the TCP policy that the TCP protocol uses.	
port-forward listname	Enters the port-forwarding submode and allows you to configure the list of ports to which the user has access. See the port-forward command for information on configuring port forwarding.	
secondary-color color	Specifies the color of the secondary title bars on the	The default color
no secondary-color	login, home, and file-access pages. See Table 2-8 for valid values.	is purple.
secondary-text-color [black white]	Specifies the color of the text on the secondary bars.	black
no secondary-text-color	It is restricted to be aligned with the title bar text color; valid values are black and white . Use the no form of this command to return to the default setting.	
ssl authenticate verify {all none}	Configures the SSL protocol uses.	all
	• authenticate verify—Specifies the SSL certificate verification method.	
	 all—Verifies all the CRLs along with signature authenticity. 	
	 none—Does not verify the certificate from the peer. 	
text-color [black white] no text-color	Specifies the color of the text on the title bars. It is restricted to just two values to limit the number of icons that need to exist for the toolbar; valid values are black and white . Use the no form of this command to return to the default setting.	white
title string	Specifies the HTML title string in the browser title	string is
no title	and on the title bar. Limited to 255 characters. Use the no form of this command to return to the default setting.	WebVPN Service.
title-color color	Specifies the color of the title bars on the login,	The default color
no title-color	home, and file-access pages. See Table 2-8 for valid values.	is purple.
username-prompt prompt	Configures the initial WebVPN login username prompt. The maximum length of prompt is 16 characters.	prompt is Login:

Table 2-7 Virtual WebVPN Context Submode Commands

Command	Purpose and Guidelines	Defaults
url-list listname	Enters the URL submode and allows you to configure the list of URLs that display on the portal Web page. See the url-list command for information on configuring the URL entries.	
vrf-name vrf-name	Specifies the VRF domain configured for the virtual WebVPN context.	

The WebVPN context links the previously configured address resolution, gateway, and authentication configurations.

To configure clientless mode, configure the URL lists and the group policy. To access email using Outlook Web Access (OWA), configure the URL list to point to the Microsoft Exchange server (for example, http://ipaddr/exchange).

To configure thin-client mode, configure the list of ports to forward and configure the group policy.

To configure file sharing using the common Internet file system (CIFS), configure the NetBIOS name service (NBNS) list, the server address, and the group policy.

Table 2-8 shows the valid values for *color* when entering the **title-color** *color* and **secondary-color** *color* commands in the WebVPN context. The default color is purple.

The value can be the name of the color that is recognized in HTML (no spaces between words or characters) or a comma-separated red, green, blue (RGB) value. The value is limited to 32 characters.



All browsers support the RGB value; however, not all browsers support the color name. If you enter a color name and do not get the expected results, use the RGB value for the color.

Table 2-8 Color Names and RGB Values

Color Name	R	G	В
AliceBlue	240	248	255
AntiqueWhite	250	235	215
AntiqueWhite1	255	239	219
AntiqueWhite2	238	223	204
AntiqueWhite3	205	192	176
AntiqueWhite4	139	131	120
Aquamarine	127	255	212
Aquamarine1	127	255	212
Aquamarine2	118	238	198
Aquamarine3	102	205	170
Aquamarine4	69	139	116
Azure	240	255	255
Azure1	240	255	255
Azure2	224	238	238

Table 2-8 Color Names and RGB Values (continued)

Azure3 193 205 205 Azure4 131 139 139 Beige 245 245 220 Bisque 255 228 196 Bisque1 255 228 196 Bisque2 238 213 183 Bisque3 205 183 158 Bisque4 139 125 107 Black 0 0 0 Blue4 0 0 255 Blue 0 0 255 Blue1 0 0 255 Blue2 0 0 205 Blue3 0 0 205 Blue4 0 0 139 BlueVolet 138 43 226 Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Burlywood4 139 35 35 <	Color Name	R	G	В
Beige 245 245 220 Bisque 255 228 196 Bisque1 255 228 196 Bisque2 238 213 183 Bisque3 205 183 158 Bisque4 139 125 107 Black 0 0 0 Black 0 0 0 Blue 0 0 255 Blue 0 0 255 Blue1 0 0 255 Blue2 0 0 238 Blue3 0 0 205 Blue4 0 0 139 Blue4 0 0 139 BlueVolet 138 43 226 Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 <	Azure3	193	205	205
Bisque 255 228 196 Bisque1 255 228 196 Bisque2 238 213 183 Bisque3 205 183 158 Bisque4 139 125 107 Black 0 0 0 Black 0 0 0 Blue 0 0 255 Blue 0 0 255 Blue1 0 0 255 Blue2 0 0 238 Blue3 0 0 205 Blue4 0 0 139 BlueViolet 138 43 226 Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145	Azure4	131	139	139
Bisque1 255 228 196 Bisque2 238 213 183 Bisque3 205 183 158 Bisque4 139 125 107 Black 0 0 0 Black 0 0 0 Blue 0 0 255 Blue 0 0 255 Blue1 0 0 255 Blue2 0 0 238 Blue3 0 0 205 Blue4 0 0 139 BlueViolet 138 43 226 Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Burlywood4 139 35 35 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125	Beige	245	245	220
Bisque2 238 213 183 Bisque3 205 183 158 Bisque4 139 125 107 Black 0 0 0 Black 0 0 0 Blue 0 0 255 Blue 0 0 255 Blue1 0 0 238 Blue2 0 0 238 Blue3 0 0 205 Blue4 0 0 139 BlueViolet 138 43 226 Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Brown4 139 35 35 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood3 205 170 125 Burlywood4 139 115 85	Bisque	255	228	196
Bisque3 205 183 158 Bisque4 139 125 107 Black 0 0 0 BlanchedAlmond 255 235 205 Blue 0 0 255 Blue 0 0 255 Blue1 0 0 238 Blue2 0 0 238 Blue3 0 0 205 Blue4 0 0 139 BlueViolet 138 43 226 Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Brown4 139 35 35 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 <	Bisque1	255	228	196
Bisque4 139 125 107 Black 0 0 0 BlanchedAlmond 255 235 205 Blue 0 0 255 Blue 1 0 0 255 Blue 2 0 0 238 Blue 3 0 0 205 Blue 4 0 0 139 Blue Violet 138 43 226 Brown 165 42 42 Brown 1 255 64 64 Brown 2 238 59 59 Brown 3 205 51 51 Brown 4 139 35 35 Burlywood 4 222 184 135 Burlywood 2 238 197 145 Burlywood 3 205 170 125 Burlywood 4 139 115 85 CadetBlue 95 158 160 CadetBlue 1 152 245 255 CadetBlue 2 142 229 <td>Bisque2</td> <td>238</td> <td>213</td> <td>183</td>	Bisque2	238	213	183
Black 0 0 0 BlanchedAlmond 255 235 205 Blue 0 0 255 Blue1 0 0 255 Blue2 0 0 238 Blue3 0 0 205 Blue4 0 0 139 BlueViolet 138 43 226 Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Brown4 139 35 35 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1	Bisque3	205	183	158
BlanchedAlmond 255 235 205 Blue 0 0 255 Blue1 0 0 255 Blue2 0 0 238 Blue3 0 0 205 Blue4 0 0 139 BlueViolet 138 43 226 Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Brown4 139 35 35 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2<	Bisque4	139	125	107
Blue 0 0 255 Blue1 0 0 255 Blue2 0 0 238 Blue3 0 0 205 Blue4 0 0 139 BlueViolet 138 43 226 Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Brown4 139 35 35 Burlywood4 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse1 127 255	Black	0	0	0
Blue1 0 0 255 Blue2 0 0 238 Blue3 0 0 205 Blue4 0 0 139 BlueViolet 138 43 226 Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Brown4 139 35 35 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue 95 158 160 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreu	BlanchedAlmond	255	235	205
Blue2 0 0 238 Blue3 0 0 205 Blue4 0 0 139 Blue Violet 138 43 226 Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Brown4 139 35 35 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse1 127 255 0 <	Blue	0	0	255
Blue3 0 0 205 Blue4 0 0 139 BlueViolet 138 43 226 Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Brown4 139 35 35 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 <td>Blue1</td> <td>0</td> <td>0</td> <td>255</td>	Blue1	0	0	255
Blue4 0 0 139 BlueViolet 138 43 226 Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Brown4 139 35 35 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	Blue2	0	0	238
BlueViolet 138 43 226 Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Brown4 139 35 35 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	Blue3	0	0	205
Brown 165 42 42 Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Brown4 139 35 35 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	Blue4	0	0	139
Brown1 255 64 64 Brown2 238 59 59 Brown3 205 51 51 Brown4 139 35 35 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	BlueViolet	138	43	226
Brown2 238 59 59 Brown3 205 51 51 Brown4 139 35 35 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	Brown	165	42	42
Brown3 205 51 51 Brown4 139 35 35 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse1 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	Brown1	255	64	64
Brown4 139 35 35 Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse1 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	Brown2	238	59	59
Burlywood 222 184 135 Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse1 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	Brown3	205	51	51
Burlywood1 255 211 155 Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse1 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	Brown4	139	35	35
Burlywood2 238 197 145 Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse1 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	Burlywood	222	184	135
Burlywood3 205 170 125 Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse1 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	Burlywood1	255	211	155
Burlywood4 139 115 85 CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse1 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	Burlywood2	238	197	145
CadetBlue 95 158 160 CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse1 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	Burlywood3	205	170	125
CadetBlue1 152 245 255 CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse1 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	Burlywood4	139	115	85
CadetBlue2 142 229 238 CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse1 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	CadetBlue	95	158	160
CadetBlue3 122 197 205 CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse1 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	CadetBlue1	152	245	255
CadetBlue4 83 134 139 Chartreuse 127 255 0 Chartreuse1 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	CadetBlue2	142	229	238
Chartreuse 127 255 0 Chartreuse1 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	CadetBlue3	122	197	205
Chartreuse1 127 255 0 Chartreuse2 118 238 0 Chartreuse3 102 205 0	CadetBlue4	83	134	139
Chartreuse2 118 238 0 Chartreuse3 102 205 0	Chartreuse	127	255	0
Chartreuse3 102 205 0	Chartreuse1	127	255	0
	Chartreuse2	118	238	0
Chartreuse4 69 139 0	Chartreuse3	102	205	0
	Chartreuse4	69	139	0

Table 2-8 Color Names and RGB Values (continued)

Color Name	R	G	В
Chocolate	210	105	30
Chocolate1	255	127	36
Chocolate2	238	118	33
Chocolate3	205	102	29
Chocolate4	139	69	19
Coral	255	127	80
Coral1	255	114	86
Coral2	238	106	80
Coral3	205	91	69
Coral4	139	62	47
CornflowerBlue	100	149	237
Cornsilk	255	248	220
Cornsilk1	255	248	220
Cornsilk2	238	232	205
Cornsilk3	205	200	177
Cornsilk4	139	136	120
Cyan	0	255	255
Cyan1	0	255	255
Cyan2	0	238	238
Cyan3	0	205	205
Cyan4	0	139	139
DarkBlue	0	0	139
DarkCyan	0	139	139
DarkGoldenrod	184	134	11
DarkGoldenrod1	255	185	15
DarkGoldenrod2	238	173	14
DarkGoldenrod3	205	149	12
DarkGoldenrod4	139	101	8
DarkGray	169	169	169
DarkGreen	0	100	0
DarkKhaki	189	183	107
DarkMagenta	139	0	139
DarkOliveGreen	85	107	47
DarkOliveGreen1	202	255	112
DarkOliveGreen2	188	238	104
DarkOliveGreen3	162	205	90

Table 2-8 Color Names and RGB Values (continued)

Color Name	R	G	В
DarkOliveGreen4	110	139	61
DarkOrange	255	140	0
DarkOrange1	255	127	0
DarkOrange2	238	118	0
DarkOrange3	205	102	0
DarkOrange4	139	69	0
DarkOrchid	153	50	204
DarkOrchid1	191	62	255
DarkOrchid2	178	58	238
DarkOrchid3	154	50	205
DarkOrchid4	104	34	139
DarkRed	139	0	0
DarkSalmon	233	150	122
DarkSeaGreen	143	188	143
DarkSeaGreen1	193	255	193
DarkSeaGreen2	180	238	180
DarkSeaGreen3	155	205	155
DarkSeaGreen4	105	139	105
DarkSlateBlue	72	61	139
DarkSlateGray	47	79	79
DarkSlateGray1	151	255	255
DarkSlateGray2	141	238	238
DarkSlateGray3	121	205	205
DarkSlateGray4	82	139	139
DarkTurquoise	0	206	209
DarkViolet	148	0	211
DeepPink	255	20	147
DeepPink1	255	20	147
DeepPink2	238	18	137
DeepPink3	205	16	118
DeepPink4	139	10	80
DeepSkyBlue	0	191	255
DeepSkyBlue1	0	191	255
DeepSkyBlue2	0	178	238
DeepSkyBlue3	0	154	205
DeepSkyBlue4	0	104	139
		-	-

Table 2-8 Color Names and RGB Values (continued)

Color Name	R	G	В
DimGrey	105	105	105
DodgerBlue	30	144	255
DodgerBlue1	30	144	255
DodgerBlue2	28	134	238
DodgerBlue3	24	116	205
DodgerBlue4	16	78	139
Firebrick	178	34	34
Firebrick1	255	48	48
Firebrick2	238	44	44
Firebrick3	205	38	38
Firebrick4	139	26	26
FloralWhite	255	250	240
ForestGreen	34	139	34
Gainsboro	220	220	220
GhostWhite	248	248	255
Gold	255	215	0
Gold1	255	215	0
Gold2	238	201	0
Gold3	205	173	0
Gold4	139	117	0
Goldenrod	218	165	32
Goldenrod1	255	193	37
Goldenrod2	238	180	34
Goldenrod3	205	155	29
Goldenrod4	139	105	20
Gray0	0	0	0
Gray1	3	3	3
Gray10	26	26	26
Gray100	255	255	255
Gray11	28	28	28
Gray12	31	31	31
Gray13	33	33	33
Gray14	36	36	36
Gray15	38	38	38
Gray16	41	41	41
Gray17	43	43	43

Table 2-8 Color Names and RGB Values (continued)

Gray18 46 46 Gray19 48 48 Gray2 5 5 Gray20 51 51 Gray21 54 54 Gray22 56 56 Gray23 59 59 Gray24 61 61 Gray25 64 64 Gray26 66 66 Ge 69 69 Gray27 69 69 Gray28 71 71 Gray29 74 74 Gray3 8 8 Gray30 77 77 Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray39 99 99 Gray4 10 10 Gray43 10 10 Gray43 10	В
Gray20 51 51 Gray21 54 54 Gray22 56 56 Gray23 59 59 Gray24 61 61 Gray25 64 64 Gray26 66 66 Gray27 69 69 Gray28 71 71 Gray29 74 74 Gray3 8 8 Gray30 77 77 Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray39 99 99 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 11	46
Gray20 51 51 Gray21 54 54 Gray22 56 56 Gray23 59 59 Gray24 61 61 Gray25 64 64 Gray26 66 66 Gray27 69 69 Gray28 71 71 Gray29 74 74 Gray3 8 8 Gray30 77 77 Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray39 99 99 Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 </td <td>48</td>	48
Gray21 54 54 Gray22 56 56 Gray23 59 59 Gray24 61 61 Gray25 64 64 Gray26 66 66 G6 66 66 Gray27 69 69 Gray28 71 71 Gray29 74 74 Gray3 8 8 Gray30 77 77 Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray4 10 10 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46	5
Gray22 56 56 Gray23 59 59 Gray24 61 61 Gray25 64 64 Gray26 66 66 G6 69 69 Gray27 69 69 Gray28 71 71 Gray29 74 74 Gray3 8 8 Gray30 77 77 Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray40 10 10 Gray41 10 10 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 <td>51</td>	51
Gray23 59 59 Gray24 61 61 Gray25 64 64 Gray26 66 66 69 69 69 Gray28 71 71 Gray29 74 74 Gray3 8 8 Gray30 77 77 Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray39 99 99 Gray4 10 10 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	54
Gray24 61 61 Gray25 64 64 Gray26 66 66 Gray27 69 69 Gray28 71 71 Gray29 74 74 Gray3 8 8 Gray30 77 77 Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray39 99 99 Gray41 10 10 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	56
Gray25 64 64 Gray26 66 66 Gray27 69 69 Gray28 71 71 Gray29 74 74 Gray3 8 8 Gray30 77 77 Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray39 99 99 Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	59
Gray26 66 66 Gray27 69 69 Gray28 71 71 Gray29 74 74 Gray3 8 8 Gray30 77 77 Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray49 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray47 120 120	61
Gray27 69 69 Gray28 71 71 Gray29 74 74 Gray3 8 8 Gray30 77 77 Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray39 99 99 Gray4 10 10 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	64
Gray28 71 71 Gray29 74 74 Gray3 8 8 Gray30 77 77 Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray39 99 99 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	66
Gray29 74 74 Gray3 8 8 Gray30 77 77 Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray39 99 99 Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	69
Gray3 8 8 Gray30 77 77 Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray39 99 99 Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	71
Gray30 77 77 Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray39 99 99 Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	74
Gray31 79 79 Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray39 99 99 Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	8
Gray32 82 82 Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray39 99 99 Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	77
Gray33 84 84 Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray39 99 99 Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	79
Gray34 87 87 Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray39 99 99 Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	82
Gray35 89 89 Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray39 99 99 Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	84
Gray36 92 92 Gray37 94 94 Gray38 97 97 Gray39 99 99 Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	87
Gray37 94 94 Gray38 97 97 Gray39 99 99 Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	89
Gray38 97 97 Gray39 99 99 Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	92
Gray39 99 99 Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	94
Gray4 10 10 Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	97
Gray40 102 102 Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	99
Gray41 105 105 Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	10
Gray42 107 107 Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	102
Gray43 110 110 Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	105
Gray44 112 112 Gray45 115 115 Gray46 117 117 Gray47 120 120	107
Gray45 115 115 Gray46 117 117 Gray47 120 120	110
Gray46 117 117 Gray47 120 120	112
Gray47 120 120	115
	117
Gray48 122 122	120
	122
Gray49 125 125	125
Gray5 13 13	13

Table 2-8 Color Names and RGB Values (continued)

Color Name	R	G	В
Gray50	127	127	127
Gray51	130	130	130
Gray52	133	133	133
Gray53	135	135	135
Gray54	138	138	138
Gray55	140	140	140
Gray56	143	143	143
Gray57	145	145	145
Gray58	148	148	148
Gray59	150	150	150
Gray6	15	15	15
Gray60	153	153	153
Gray61	156	156	156
Gray62	158	158	158
Gray63	161	161	161
Gray64	163	163	163
Gray65	166	166	166
Gray66	168	168	168
Gray67	171	171	171
Gray68	173	173	173
Gray69	176	176	176
Gray7	18	18	18
Gray70	179	179	179
Gray71	181	181	181
Gray72	184	184	184
Gray73	186	186	186
Gray74	189	189	189
Gray75	191	191	191
Gray76	194	194	194
Gray77	196	196	196
Gray78	199	199	199
Gray79	201	201	201
Gray8	20	20	20
Gray80	204	204	204
Gray81	207	207	207
Gray82	209	209	209

Table 2-8 Color Names and RGB Values (continued)

Gray84 212 212 212 212 Gray84 214 214 214 214 214 214 214 214 214 214 214 214 214 214 214 214 214 217 227 229 229 229 229 229 229 229 229 229	Color Name	R	G	В
Gray86 217 217 217 217 Gray86 219 219 219 219 Gray87 222 222 222 222 Gray88 224 224 224 224 Gray99 23 23 23 23 Gray90 229 229 229 229 Gray91 232 232 232 232 Gray92 235 235 235 235 Gray92 235 235 235 235 Gray93 237 237 237 237 Gray94 240 240 240 240 240 240 240 240 242 242 242 242 242 242 242 242 242 242 242 242 242 242 242 244 247 247 247 247 247 247 247 247 247 247 247 <t< td=""><td>Gray83</td><td>212</td><td>212</td><td>212</td></t<>	Gray83	212	212	212
Gray86 219 219 219 Gray87 222 222 222 Gray88 224 224 224 Gray89 227 227 227 Gray9 23 23 23 Gray90 229 229 229 Gray91 232 232 232 Gray92 235 235 235 Gray93 237 237 237 Gray94 240 240 240 Gray95 242 242 242 Gray96 245 245 245 Gray97 247 247 247 Gray98 250 250 250 Green 0 255 0 Green1 0 255 0 Green 0 255 0 Green 0 238 0 Green 0 238 0 Green 0	Gray84	214	214	214
Gray87 222 222 222 Gray88 224 224 224 Gray89 227 227 227 Gray9 23 23 23 Gray90 229 229 229 Gray91 232 232 232 Gray92 235 235 235 Gray93 237 237 237 Gray94 240 240 240 Gray95 242 242 242 Gray96 245 245 245 Gray97 247 247 247 Gray98 250 250 250 Green 0 255 0 Green 0 255 0 Green 0 255 0 Green 0 238 0 Green 0 205 0 Green 0 205 0 Grey0 0 0	Gray85	217	217	217
Gray88 224 224 224 Gray89 227 227 227 Gray9 23 23 23 Gray90 229 229 229 Gray91 232 232 232 Gray92 235 235 235 Gray93 237 237 237 Gray94 240 240 240 Gray95 242 242 242 Gray96 245 245 245 Gray97 247 247 247 Gray98 250 250 250 Green 0 255 0 Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 Grey0 0 0 0 Grey1 3 3 3 Grey10 26 26 </td <td>Gray86</td> <td>219</td> <td>219</td> <td>219</td>	Gray86	219	219	219
Gray89 227 227 227 Gray9 23 23 23 Gray90 229 229 229 Gray91 232 232 232 Gray92 235 235 235 Gray93 237 237 237 Gray94 240 240 240 Gray95 242 242 242 Gray96 245 245 245 Gray97 247 247 247 Gray98 250 250 250 Green 0 255 0 Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 Grey0 0 0 0 Grey1 3 3 3 Grey10 26 26 26 Grey12 31 31	Gray87	222	222	222
Gray9 23 23 23 Gray90 229 229 229 Gray91 232 232 232 Gray92 235 235 235 Gray93 237 237 237 Gray94 240 240 240 Gray95 242 242 242 Gray96 245 245 245 Gray97 247 247 247 Gray98 250 250 250 Green 0 255 0 Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 GreenYellow 173 255 47 Grey0 0 0 0 Grey1 3 3 3 Grey10 26 26 26 Ge 26 26	Gray88	224	224	224
Gray90 229 229 229 Gray91 232 232 232 Gray92 235 235 235 Gray93 237 237 237 Gray94 240 240 240 Gray95 242 242 242 Gray96 245 245 245 Gray97 247 247 247 Gray98 250 250 250 Gray99 252 252 252 Green 0 255 0 Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 Grey0 0 0 0 Grey1 3 3 3 Grey10 26 26 26 Gey10 255 255 255 Grey13 33 33 </td <td>Gray89</td> <td>227</td> <td>227</td> <td>227</td>	Gray89	227	227	227
Gray91 232 232 232 Gray92 235 235 235 Gray93 237 237 237 Gray94 240 240 240 Gray95 242 242 242 Gray96 245 245 245 Gray97 247 247 247 Gray98 250 250 250 Green 0 255 0 Green 0 255 0 Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 Grey 190 190 190 Grey 190 190 190 Grey1 3 3 3 Grey10 26 26 26 Grey11 28 28 28 Grey13 33 33	Gray9	23	23	23
Gray92 235 235 235 Gray93 237 237 237 Gray94 240 240 240 Gray95 242 242 242 Gray96 245 245 245 Gray97 247 247 247 Gray98 250 250 250 Gray99 252 252 252 Green 0 255 0 Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 Grey10w 173 255 47 Grey 190 190 190 Grey1 3 3 3 Grey10 26 26 26 Grey100 255 255 255 Grey11 28 28 28 Grey13 33 33 33 Grey14 36 36 36 <t< td=""><td>Gray90</td><td>229</td><td>229</td><td>229</td></t<>	Gray90	229	229	229
Gray93 237 237 237 Gray94 240 240 240 Gray95 242 242 242 Gray96 245 245 245 Gray97 247 247 247 Gray98 250 250 250 Green 0 255 0 Green 0 255 0 Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 GreenYellow 173 255 47 Grey 190 190 190 Grey1 3 3 3 Grey10 26 26 26 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36	Gray91	232	232	232
Gray94 240 240 240 Gray95 242 242 242 Gray96 245 245 245 Gray97 247 247 247 Gray98 250 250 250 Gray99 252 252 252 Green 0 255 0 Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 Grey 190 190 190 190 Grey 1 3 3 3 Grey 10 26 26 26 Grey 10 255 255 255 Grey 11 28 28 28 Grey 12 31 31 31 Grey 13 36 36 36 Grey 15 38 38 38 Grey 16 41 <t< td=""><td>Gray92</td><td>235</td><td>235</td><td>235</td></t<>	Gray92	235	235	235
Gray95 242 242 242 Gray96 245 245 245 Gray97 247 247 247 Gray98 250 250 250 Gray99 252 252 252 Green 0 255 0 Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 GreenYellow 173 255 47 Grey 190 190 190 Grey0 0 0 0 Grey1 3 3 3 Grey10 26 26 26 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38	Gray93	237	237	237
Gray96 245 245 245 Gray97 247 247 247 Gray98 250 250 250 Gray99 252 252 252 Green 0 255 0 Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 GreenYellow 173 255 47 Grey 190 190 190 Grey0 0 0 0 Grey1 3 3 3 Grey100 255 255 255 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Gray94	240	240	240
Gray97 247 247 247 Gray98 250 250 250 Gray99 252 252 252 Green 0 255 0 Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 Grey 100 190 190 190 Grey 1 3 3 3 Grey 10 26 26 26 Grey 100 255 255 255 Grey 11 28 28 28 Grey 12 31 31 31 Grey 13 33 33 33 Grey 14 36 36 36 Grey 15 38 38 38 Grey 16 41 41 41	Gray95	242	242	242
Gray98 250 250 250 Gray99 252 252 252 Green 0 255 0 Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 Grey Holow 173 255 47 Grey 190 190 190 Grey0 0 0 0 Grey1 3 3 3 Grey100 26 26 26 26 Grey10 255 255 255 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Gray96	245	245	245
Gray99 252 252 252 Green 0 255 0 Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 Grey Holo 173 255 47 Grey 190 190 190 Grey0 0 0 0 Grey1 3 3 3 Grey100 26 26 26 Grey10 255 255 255 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey15 38 38 38 Grey16 41 41 41	Gray97	247	247	247
Green 0 255 0 Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 GreenYellow 173 255 47 Grey 190 190 190 Grey0 0 0 0 Grey1 3 3 3 Grey100 255 255 255 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Gray98	250	250	250
Green1 0 255 0 Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 Green Yellow 173 255 47 Grey 190 190 190 Grey0 0 0 0 Grey1 3 3 3 Grey100 26 26 26 Grey100 255 255 255 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Gray99	252	252	252
Green2 0 238 0 Green3 0 205 0 Green4 0 139 0 GreenYellow 173 255 47 Grey 190 190 190 Grey0 0 0 0 Grey1 3 3 3 Grey10 26 26 26 Grey100 255 255 255 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Green	0	255	0
Green3 0 205 0 Green4 0 139 0 GreenYellow 173 255 47 Grey 190 190 190 Grey0 0 0 0 Grey1 3 3 3 Grey10 26 26 26 Grey100 255 255 255 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Green1	0	255	0
Green4 0 139 0 GreenYellow 173 255 47 Grey 190 190 190 Grey0 0 0 0 Grey1 3 3 3 Grey10 26 26 26 Grey100 255 255 255 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Green2	0	238	0
GreenYellow 173 255 47 Grey 190 190 190 Grey0 0 0 0 Grey1 3 3 3 Grey10 26 26 26 Grey100 255 255 255 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Green3	0	205	0
Grey 190 190 190 Grey0 0 0 0 Grey1 3 3 3 Grey10 26 26 26 Grey100 255 255 255 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Green4	0	139	0
Grey0 0 0 Grey1 3 3 Grey10 26 26 26 Grey100 255 255 255 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	GreenYellow	173	255	47
Grey1 3 3 Grey10 26 26 26 Grey100 255 255 255 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Grey	190	190	190
Grey10 26 26 26 Grey100 255 255 255 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Grey0	0	0	0
Grey100 255 255 255 Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Grey1	3	3	3
Grey11 28 28 28 Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Grey10	26	26	26
Grey12 31 31 31 Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Grey100	255	255	255
Grey13 33 33 33 Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Grey11	28	28	28
Grey14 36 36 36 Grey15 38 38 38 Grey16 41 41 41	Grey12	31	31	31
Grey15 38 38 38 Grey16 41 41 41	Grey13	33	33	33
Grey16 41 41 41	Grey14	36	36	36
	Grey15	38	38	38
Grey17 43 43 43	Grey16	41	41	41
	Grey17	43	43	43

Table 2-8 Color Names and RGB Values (continued)

Color Name	R	G	В
Grey18	46	46	46
Grey19	48	48	48
Grey2	5	5	5
Grey20	51	51	51
Grey21	54	54	54
Grey22	56	56	56
Grey23	59	59	59
Grey24	61	61	61
Grey25	64	64	64
Grey26	66	66	66
Grey27	69	69	69
Grey28	71	71	71
Grey29	74	74	74
Grey3	8	8	8
Grey30	77	77	77
Grey31	79	79	79
Grey32	82	82	82
Grey33	84	84	84
Grey34	87	87	87
Grey35	89	89	89
Grey36	92	92	92
Grey37	94	94	94
Grey38	97	97	97
Grey39	99	99	99
Grey4	10	10	10
Grey40	102	102	102
Grey41	105	105	105
Grey42	107	107	107
Grey43	110	110	110
Grey44	112	112	112
Grey45	115	115	115
Grey46	117	117	117
Grey47	120	120	120
Grey48	122	122	122
Grey49	125	125	125
Grey5	13	13	13

Table 2-8 Color Names and RGB Values (continued)

Grey50 127 127 127 Grey51 130 130 130 Grey52 133 133 133 Grey53 135 135 135 Grey54 138 138 138 Grey55 140 140 140 Grey56 143 143 143 Grey57 145 145 145 Grey58 148 148 148 Grey59 150 150 150 Grey6 15 15 15 Grey60 153 153 153 Grey61 156 156 156 Grey62 158 158 158 Grey63 161 161 161 Grey64 163 163 163 Grey65 166 166 166 Grey66 168 168 168 Grey70 171 171 171 171	Color Name	R	G	В
Grey52 133 133 133 Grey53 135 135 135 Grey54 138 138 138 Grey55 140 140 140 Grey56 143 143 143 Grey57 145 145 145 Grey58 148 148 148 Grey59 150 150 150 Grey6 15 15 15 Grey60 153 153 153 Grey61 156 156 156 Grey62 158 158 158 Grey63 161 161 161 Grey64 163 163 163 Grey65 166 166 166 Grey66 168 168 168 Grey69 176 176 176 Grey70 179 179 179 Grey71 181 181 181 Grey72	Grey50	127	127	127
Grey53 135 135 135 Grey54 138 138 138 Grey55 140 140 140 Grey56 143 143 143 143 Grey57 145 145 145 145 Grey58 148 148 148 148 Grey59 150 150 150 150 Grey6 15 15 15 15 Grey6 153 153 153 153 Grey60 153 153 153 153 Grey61 156 156 156 156 Grey62 158 158 158 158 Grey63 161 161 161 161 161 161 161 161 163 163 163 163 163 163 163 163 163 163 163 163 163 163 163 163 163 163 <t< td=""><td>Grey51</td><td>130</td><td>130</td><td>130</td></t<>	Grey51	130	130	130
Grey54 138 138 138 Grey55 140 140 140 Grey56 143 143 143 Grey57 145 145 145 Grey58 148 148 148 Grey59 150 150 150 Grey6 15 15 15 Grey60 153 153 153 Grey61 156 156 156 Grey62 158 158 158 Grey63 161 161 161 Grey64 163 163 163 Grey65 166 166 166 Grey66 168 168 168 Grey67 171 171 171 Grey68 173 173 173 Grey7 18 18 18 Grey7 18 18 18 Grey70 179 179 179 Grey72 <	Grey52	133	133	133
Grey55 140 140 140 Grey56 143 143 143 Grey57 145 145 145 Grey58 148 148 148 Grey59 150 150 150 Grey6 15 15 15 Grey60 153 153 153 Grey61 156 156 156 Grey61 156 156 156 Grey62 158 158 158 Grey63 161 161 161 Grey63 163 163 163 Grey64 163 163 163 Grey65 166 166 166 Grey66 168 168 168 Grey67 171 171 171 Grey68 173 173 173 Grey7 18 18 18 Grey7 18 18 18 Grey71 <	Grey53	135	135	135
Grey56 143 143 143 Grey57 145 145 145 Grey58 148 148 148 Grey59 150 150 150 Grey6 15 15 15 Grey60 153 153 153 Grey61 156 156 156 Grey62 158 158 158 Grey63 161 161 161 161 Grey64 163 163 163 163 Grey65 166 166 166 166 Grey66 168 168 168 168 Grey67 171 171 171 171 171 Grey68 173 173 173 173 173 173 173 173 179 179 179 179 179 179 179 179 179 179 179 179 179 179 184 184	Grey54	138	138	138
Grey57 145 145 145 Grey58 148 148 148 Grey59 150 150 150 Grey6 15 15 15 Grey60 153 153 153 Grey61 156 156 156 Grey62 158 158 158 Grey63 161 161 161 Grey64 163 163 163 Grey65 166 166 166 Grey66 168 168 168 Grey67 171 171 171 Grey68 173 173 173 Grey69 176 176 176 Grey7 18 18 18 Grey7 18 18 18 Grey70 179 179 179 Grey71 181 181 181 Grey72 184 184 184 Grey73 <	Grey55	140	140	140
Grey58 148 148 148 Grey59 150 150 150 Grey6 15 15 15 Grey60 153 153 153 Grey61 156 156 156 Grey62 158 158 158 Grey63 161 161 161 Grey64 163 163 163 Grey65 166 166 166 Grey66 168 168 168 Grey67 171 171 171 171 Grey69 176 176 176 176 Grey7 18 18 18 18 Grey7 18 18 18 18 Grey70 179 179 179 179 Grey71 181 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Gre	Grey56	143	143	143
Grey59 150 150 150 Grey6 15 15 15 Grey60 153 153 153 Grey61 156 156 156 Grey62 158 158 158 Grey63 161 161 161 Grey63 163 163 163 Grey64 163 163 163 Grey65 166 166 166 Grey66 168 168 168 Grey67 171 171 171 Grey68 173 173 173 Grey7 18 18 18 Grey7 18 18 18 Grey7 181 181 181 Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 <t< td=""><td>Grey57</td><td>145</td><td>145</td><td>145</td></t<>	Grey57	145	145	145
Grey60 15 15 153 Grey61 156 156 156 Grey62 158 158 158 Grey63 161 161 161 Grey64 163 163 163 Grey65 166 166 166 Grey66 168 168 168 Grey67 171 171 171 Grey68 173 173 173 Grey69 176 176 176 Grey7 18 18 18 Grey70 179 179 179 Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey77 196 196 196 Grey79	Grey58	148	148	148
Grey60 153 153 153 Grey61 156 156 156 Grey62 158 158 158 Grey63 161 161 161 Grey64 163 163 163 Grey65 166 166 166 Grey66 168 168 168 Grey67 171 171 171 Grey68 173 173 173 Grey69 176 176 176 Grey7 18 18 18 Grey70 179 179 179 Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey78 199 199 199 Grey8	Grey59	150	150	150
Grey61 156 156 156 Grey62 158 158 158 Grey63 161 161 161 Grey64 163 163 163 Grey65 166 166 166 Grey66 168 168 168 Grey67 171 171 171 Grey68 173 173 173 Grey69 176 176 176 Grey7 18 18 18 Grey70 179 179 179 Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey77 196 196 196 Grey79 201 201 201 Grey80	Grey6	15	15	15
Grey62 158 158 158 Grey63 161 161 161 Grey64 163 163 163 Grey65 166 166 166 Grey66 168 168 168 Grey67 171 171 171 Grey68 173 173 173 Grey7 18 18 18 Grey7 18 18 18 Grey70 179 179 179 Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey78 199 199 199 Grey79 201 201 201 Grey80 204 204 204 Grey81 207 207 207	Grey60	153	153	153
Grey63 161 161 161 Grey64 163 163 163 Grey65 166 166 166 Grey66 168 168 168 Grey67 171 171 171 Grey68 173 173 173 Grey69 176 176 176 Grey7 18 18 18 Grey70 179 179 179 Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey78 199 199 199 Grey79 201 201 201 Grey80 204 204 204 Grey81 207 207 207	Grey61	156	156	156
Grey64 163 163 163 Grey65 166 166 166 Grey66 168 168 168 Grey67 171 171 171 Grey68 173 173 173 Grey69 176 176 176 Grey7 18 18 18 Grey70 179 179 179 Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey78 199 199 199 Grey79 201 201 201 Grey80 204 204 204 Grey81 207 207 207	Grey62	158	158	158
Grey65 166 166 166 Grey66 168 168 168 Grey67 171 171 171 Grey68 173 173 173 Grey69 176 176 176 Grey7 18 18 18 Grey70 179 179 179 Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey77 196 196 196 Grey79 201 201 201 Grey80 204 204 204 Grey81 207 207 207	Grey63	161	161	161
Grey66 168 168 168 Grey67 171 171 171 Grey68 173 173 173 Grey69 176 176 176 Grey7 18 18 18 Grey70 179 179 179 Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey78 199 199 199 Grey79 201 201 201 Grey80 204 204 204 Grey81 207 207 207	Grey64	163	163	163
Grey67 171 171 171 Grey68 173 173 173 Grey69 176 176 176 Grey7 18 18 18 Grey70 179 179 179 Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey78 199 199 199 Grey79 201 201 201 Grey80 20 20 20 Grey81 207 207 207	Grey65	166	166	166
Grey68 173 173 173 Grey69 176 176 176 Grey7 18 18 18 Grey70 179 179 179 Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey77 196 196 196 Grey79 201 201 201 Grey80 20 20 20 Grey81 207 207 207	Grey66	168	168	168
Grey69 176 176 176 Grey7 18 18 18 Grey70 179 179 179 Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 191 Grey76 194 194 194 194 Grey77 196 196 196 196 Grey78 199 199 199 199 Grey8 20 20 20 Grey80 204 204 204 Grey81 207 207 207	Grey67	171	171	171
Grey7 18 18 18 Grey70 179 179 179 Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey77 196 196 196 Grey78 199 199 199 Grey79 201 201 201 Grey80 204 204 204 Grey81 207 207 207	Grey68	173	173	173
Grey70 179 179 179 Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey77 196 196 196 Grey78 199 199 199 Grey79 201 201 201 Grey80 204 204 204 Grey81 207 207 207	Grey69	176	176	176
Grey71 181 181 181 Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey77 196 196 196 Grey78 199 199 199 Grey79 201 201 201 Grey8 20 20 20 Grey80 204 204 204 Grey81 207 207 207	Grey7	18	18	18
Grey72 184 184 184 Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey77 196 196 196 Grey78 199 199 199 Grey79 201 201 201 Grey8 20 20 20 Grey80 204 204 204 Grey81 207 207 207	Grey70	179	179	179
Grey73 186 186 186 Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey77 196 196 196 Grey78 199 199 199 Grey79 201 201 201 Grey8 20 20 20 Grey80 204 204 204 Grey81 207 207 207	Grey71	181	181	181
Grey74 189 189 189 Grey75 191 191 191 Grey76 194 194 194 Grey77 196 196 196 Grey78 199 199 199 Grey79 201 201 201 Grey8 20 20 20 Grey80 204 204 204 Grey81 207 207 207	Grey72	184	184	184
Grey75 191 191 191 Grey76 194 194 194 Grey77 196 196 196 Grey78 199 199 199 Grey79 201 201 201 Grey8 20 20 20 Grey80 204 204 204 Grey81 207 207 207	Grey73	186	186	186
Grey76 194 194 194 Grey77 196 196 196 Grey78 199 199 199 Grey79 201 201 201 Grey8 20 20 20 Grey80 204 204 204 Grey81 207 207 207	Grey74	189	189	189
Grey77 196 196 196 Grey78 199 199 199 Grey79 201 201 201 Grey8 20 20 20 Grey80 204 204 204 Grey81 207 207 207	Grey75	191	191	191
Grey78 199 199 199 Grey79 201 201 201 Grey8 20 20 20 Grey80 204 204 204 Grey81 207 207 207	Grey76	194	194	194
Grey79 201 201 201 Grey8 20 20 20 Grey80 204 204 204 Grey81 207 207 207	Grey77	196	196	196
Grey8 20 20 20 Grey80 204 204 204 Grey81 207 207 207	Grey78	199	199	199
Grey80 204 204 204 Grey81 207 207 207	Grey79	201	201	201
Grey81 207 207 207	Grey8	20	20	20
	Grey80	204	204	204
Grey82 209 209 209	Grey81	207	207	207
	Grey82	209	209	209

Table 2-8 Color Names and RGB Values (continued)

Color Name	R	G	В
Grey83	212	212	212
Grey84	214	214	214
Grey85	217	217	217
Grey86	219	219	219
Grey87	222	222	222
Grey88	224	224	224
Grey89	227	227	227
Grey9	23	23	23
Grey90	229	229	229
Grey91	232	232	232
Grey92	235	235	235
Grey93	237	237	237
Grey94	240	240	240
Grey95	242	242	242
Grey96	245	245	245
Grey97	247	247	247
Grey98	250	250	250
Grey99	252	252	252
Honeydew	240	255	240
Honeydew1	240	255	240
Honeydew2	224	238	224
Honeydew3	193	205	193
Honeydew4	131	139	131
HotPink	255	105	180
HotPink1	255	110	180
HotPink2	238	106	167
HotPink3	205	96	144
HotPink4	139	58	98
IndianRed	205	92	92
IndianRed1	255	106	106
IndianRed2	238	99	99
IndianRed3	205	85	85
IndianRed4	139	58	58
Ivory	255	255	240
Ivory1	255	255	240
Ivory2	238	238	224

Table 2-8 Color Names and RGB Values (continued)

Color Name	R	G	В
Ivory3	205	205	193
Ivory4	139	139	131
Khaki	240	230	140
Khaki1	255	246	143
Khaki2	238	230	133
Khaki3	205	198	115
Khaki4	139	134	78
Lavender	230	230	250
LavenderBlush	255	240	245
LavenderBlush1	255	240	245
LavenderBlush2	238	224	229
LavenderBlush3	205	193	197
LavenderBlush4	139	131	134
LawnGreen	124	252	0
LemonChiffon	255	250	205
LemonChiffon1	255	250	205
LemonChiffon2	238	233	191
LemonChiffon3	205	201	165
LemonChiffon4	139	137	112
LightBlue	173	216	230
LightBlue1	191	239	255
LightBlue2	178	223	238
LightBlue3	154	192	205
LightBlue4	104	131	139
LightCoral	240	128	128
LightCyan	224	255	255
LightCyan1	224	255	255
LightCyan2	209	238	238
LightCyan3	180	205	205
LightCyan4	122	139	139
LightGoldenrod	238	221	130
LightGoldenrod1	255	236	139
LightGoldenrod2	238	220	130
LightGoldenrod3	205	190	112
LightGoldenrod4	139	129	76
LightGoldenrodYellow	250	250	210

Table 2-8 Color Names and RGB Values (continued)

Color Name	R	G	В
LightGreen	144	238	144
LightGrey	211	211	211
LightPink	255	182	193
LightPink1	255	174	185
LightPink2	238	162	173
LightPink3	205	140	149
LightPink4	139	95	101
LightSalmon	255	160	122
LightSalmon1	255	160	122
LightSalmon2	238	149	114
LightSalmon3	205	129	98
LightSalmon4	139	87	66
LightSeaGreen	32	178	170
LightSkyBlue	135	206	250
LightSkyBlue1	176	226	255
LightSkyBlue2	164	211	238
LightSkyBlue3	141	182	205
LightSkyBlue4	96	123	139
LightSlateBlue	132	112	255
LightSlateGray	119	136	153
LightSteelBlue	176	196	222
LightSteelBlue1	202	225	255
LightSteelBlue2	188	210	238
LightSteelBlue3	162	181	205
LightSteelBlue4	110	123	139
LightYellow	255	255	224
LightYellow1	255	255	224
LightYellow2	238	238	209
LightYellow3	205	205	180
LightYellow4	139	139	122
LimeGreen	50	205	50
Linen	250	240	230
Magenta	255	0	255
Magenta1	255	0	255
Magenta2	238	0	238
Magenta3	205	0	205

Table 2-8 Color Names and RGB Values (continued)

Color Name	R	G	В
Magenta4	139	0	139
Maroon	176	48	96
Maroon1	255	52	179
Maroon2	238	48	167
Maroon3	205	41	144
Maroon4	139	28	98
MediumAquamarine	102	205	170
MediumBlue	0	0	205
MediumOrchid	186	85	211
MediumOrchid1	224	102	255
MediumOrchid2	209	95	238
MediumOrchid3	180	82	205
MediumOrchid4	122	55	139
MediumPurple	147	112	219
MediumPurple1	171	130	255
MediumPurple2	159	121	238
MediumPurple3	137	104	205
MediumPurple4	93	71	139
MediumSeaGreen	60	179	113
MediumSlateBlue	123	104	238
MediumSpringGreen	0	250	154
MediumTurquoise	72	209	204
MediumVioletRed	199	21	133
MidnightBlue	25	25	112
MintCream	245	255	250
MistyRose	255	228	225
MistyRose1	255	228	225
MistyRose2	238	213	210
MistyRose3	205	183	181
MistyRose4	139	125	123
Moccasin	255	228	181
NavajoWhite	255	222	173
NavajoWhite1	255	222	173
NavajoWhite2	238	207	161
NavajoWhite3	205	179	139
NavajoWhite4	139	121	94

Table 2-8 Color Names and RGB Values (continued)

Color Name	R	G	В
Navy	0	0	128
NavyBlue	0	0	128
OldLace	253	245	230
OliveDrab	107	142	35
OliveDrab1	192	255	62
OliveDrab2	179	238	58
OliveDrab3	154	205	50
OliveDrab4	105	139	34
Orange	255	165	0
Orange1	255	165	0
Orange2	238	154	0
Orange3	205	133	0
Orange4	139	90	0
OrangeRed	255	69	0
OrangeRed1	255	69	0
OrangeRed2	238	64	0
OrangeRed3	205	55	0
OrangeRed4	139	37	0
Orchid	218	112	214
Orchid1	255	131	250
Orchid2	238	122	233
Orchid3	205	105	201
Orchid4	139	71	137
PaleGoldenrod	238	232	170
PaleGreen	152	251	152
PaleGreen1	154	255	154
PaleGreen2	144	238	144
PaleGreen3	124	205	124
PaleGreen4	84	139	84
PaleTurquoise	175	238	238
PaleTurquoise1	187	255	255
PaleTurquoise2	174	238	238
PaleTurquoise3	150	205	205
PaleTurquoise4	102	139	139
PaleVioletRed	219	112	147
PaleVioletRed1	255	130	171

Table 2-8 Color Names and RGB Values (continued)

Color Name	R	G	В
PaleVioletRed2	238	121	159
PaleVioletRed3	205	104	137
PaleVioletRed4	139	71	93
PapayaWhip	255	239	213
PeachPuff	255	218	185
PeachPuff1	255	218	185
PeachPuff2	238	203	173
PeachPuff3	205	175	149
PeachPuff4	139	119	101
Peru	205	133	63
Pink	255	192	203
Pink1	255	181	197
Pink2	238	169	184
Pink3	205	145	158
Pink4	139	99	108
Plum	221	160	221
Plum1	255	187	255
Plum2	238	174	238
Plum3	205	150	205
Plum4	139	102	139
PowderBlue	176	224	230
Purple	160	32	240
Purple1	155	48	255
Purple2	145	44	238
Purple3	125	38	205
Purple4	85	26	139
Red	255	0	0
Red1	255	0	0
Red2	238	0	0
Red3	205	0	0
Red4	139	0	0
RosyBrown	188	143	143
RosyBrown1	255	193	193
RosyBrown2	238	180	180
RosyBrown3	205	155	155
RosyBrown4	139	105	105

Table 2-8 Color Names and RGB Values (continued)

Color Name	R	G	В
RoyalBlue	65	105	225
RoyalBlue1	72	118	255
RoyalBlue2	67	110	238
RoyalBlue3	58	95	205
RoyalBlue4	39	64	139
SaddleBrown	139	69	19
Salmon	250	128	114
Salmon1	255	140	105
Salmon2	238	130	98
Salmon3	205	112	84
Salmon4	139	76	57
SandyBrown	244	164	96
SeaGreen	46	139	87
SeaGreen1	84	255	159
SeaGreen2	78	238	148
SeaGreen3	67	205	128
SeaGreen4	46	139	87
Seashell	255	245	238
Seashell1	255	245	238
Seashell2	238	229	222
Seashell3	205	197	191
Seashell4	139	134	130
Sienna	160	82	45
Sienna1	255	130	71
Sienna2	238	121	66
Sienna3	205	104	57
Sienna4	139	71	38
SkyBlue	135	206	235
SkyBlue1	135	206	255
SkyBlue2	126	192	238
SkyBlue3	108	166	205
SkyBlue4	74	112	139
SlateBlue	106	90	205
SlateBlue1	131	111	255
SlateBlue2	122	103	238
SlateBlue3	105	89	205

Table 2-8 Color Names and RGB Values (continued)

Color Name	R	G	В
SlateBlue4	71	60	139
SlateGray	112	128	144
SlateGray1	198	226	255
SlateGray2	185	211	238
SlateGray3	159	182	205
SlateGray4	108	123	139
Snow	255	250	250
Snow1	255	250	250
Snow2	238	233	233
Snow3	205	201	201
Snow4	139	137	137
SpringGreen	0	255	127
SpringGreen1	0	255	127
SpringGreen2	0	238	118
SpringGreen3	0	205	102
SpringGreen4	0	139	69
SteelBlue	70	130	180
SteelBlue1	99	184	255
SteelBlue2	92	172	238
SteelBlue3	79	148	205
SteelBlue4	54	100	139
Tan	210	180	140
Tan1	255	165	79
Tan2	238	154	73
Tan3	205	133	63
Tan4	139	90	43
Thistle	216	191	216
Thistle1	255	225	255
Thistle2	238	210	238
Thistle3	205	181	205
Thistle4	139	123	139
Tomato	255	99	71
Tomato1	255	99	71
Tomato2	238	92	66
Tomato3	205	79	57
Tomato4	139	54	38

Table 2-8 Color Names and RGB Values (continued)

Color Name	R	G	В
Turquoise	64	224	208
Turquoise1	0	245	255
Turquoise2	0	229	238
Turquoise3	0	197	205
Turquoise4	0	134	139
Violet	238	130	238
VioletRed	208	32	144
VioletRed1	255	62	150
VioletRed2	238	58	140
VioletRed3	205	50	120
VioletRed4	139	34	82
Wheat	245	222	179
Wheat1	255	231	186
Wheat2	238	216	174
Wheat3	205	186	150
Wheat4	139	126	102
White	255	255	255
WhiteSmoke	245	245	245
Yellow	255	255	0
Yellow1	255	255	0
Yellow2	238	238	0
Yellow3	205	205	0
Yellow4	139	139	0
YellowGreen	154	205	50

Examples

This example shows how to enter the WebVPN context submode and define the virtual WebVPN context:

```
webvpn(config)# webvpn context cisco
webvpn(config-webvpn-context)# url-list cisco
webvpn(config-webvpn-url)# url-text cisco url-value http://cisco.com
webvpn(config-webvpn-url)# url-text CNN url-value http://cnn.com
webvpn(config-webvpn-url)# url-text yahoo url-value http://yahoo.com
webvpn(config-webvpn-url)# exit
webvpn(config-webvpn-context)#
```

```
webvpn(config-webvpn-context)# policy group cisco
webvpn(config-webvpn-group)# url-list cisco
webvpn(config-webvpn-group)# nat-address 172.21.65.73 172.21.65.78 netmask 255.0.0.0
webvpn(config-webvpn-group)# exit
webvpn(config-webvpn-context)# default-group-policy cisco
webvpn(config-webvpn-context)# aaa authentication test
webvpn(config-webvpn-context)# gateway common
webvpn(config-webvpn-context)# inservice
webvpn(config-webvpn-context)# end
webvpn#
```

webvpn gateway

To enter the gateway submode and define the virtual gateway, use the **webvpn gateway** command. Use the **no** form of this command to remove any commands that you have entered in the WebVPN subcommand mode from the configuration.

webvpn gateway gateway-name

Syntax Description	gateway-name	Name of the virtual gateway service.
Defaults	This command has r	no default settings.
Command Modes	Global configuration	1
Command History	Release	Modification
	WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

The gateway-name argument is case-sensitive.

After you enter the webvpn gateway command, the prompt changes to the following:

webvpn(config-webvpn-gateway)#

After you enter the gateway submode, there are commands available to configure the virtual gateway services. Table 2-9 lists the virtual gateway submode commands.

Table 2-9 Virtual Gateway Submode Commands

Command	Purpose and Guidelines	Defaults
exit	Exits from the gateway configuration mode and returns to the global configuration mode.	
hostname hostname	Specifies the name of the gateway that is used in the URL and cookie mangling process. In the load-balancing configuration, the hostname specified here is the virtual gateway IP address configured on the LB device.	
http-redirect [port port]	Specifies that the HTTP port is open and that any HTTP connections to the virtual gateway is directed to use secure HTTP (HTTPS). port port—(Optional) Specifies the port number to be redirected; valid values are from 1 to 65535.	port is 80.
inservice no inservice	Enables the WebVPN gateway. Use the no form of this command to disable the WebVPN gateway.	

Table 2-9 Virtual Gateway Submode Commands (continued)

Command	Purpose and Guidelines	Defaults
<pre>ip address ip-addr [netmask][port port] [secondary]</pre>	Defines the virtual IP address for which the WebVPN Services Module is the proxy.	port is 443 .
	• port <i>port</i> —(Optional) Specifies the port number for which the WebVPN Services Module is the proxy; valid values are from 1 to 65535.	
	• secondary —(Optional) Configures the gateway as the secondary IP. The secondary keyword is required if the virtual IP address is not on a network with a direct connection.	
policy tcp tcp-policy-name no policy tcp	(Optional) Specifies the TCP policy to use. Use the no form of this command to return to the default policy.	
policy ssl ssl-policy-name no policy ssl	(Optional) Specifies the SSL policy to use. Use the no form of this command to return to the default policy.	
ssl trustpoint trustpoint-label	Applies a trustpoint configuration to the WebVPN gateway. You can import the test certificate embedded on the module.	
	Note The trustpoint defines the certificate authority server, the key parameters and key-generation methods, and the certificate enrollment methods for the WebVPN gateway.	

To configure the mask address to specify a wildcard proxy service, use the **ip address** *ip-addr* command and use these guidelines:

- You must enter the **secondary** keyword to configure a wildcard proxy service.
- When you enter the secondary keyword, the WebVPN Services Module does not respond to ARP requests of the virtual IP address.
- You can enter the **secondary** keyword when the WebVPN Services Module is used in a standalone configuration or when the WebVPN Services Module is used as a real server on a load balancer (such as the CSM) configured in dispatch mode (MAC address rewrite).
- You can enter the secondary keyword if you configure multiple devices using the same virtual IP address. The virtual IP address can be any legal IP address, and does not have to be in the VLAN (subnet) connected to the WebVPN Services Module.

If you create a policy by entering the **webvpn policy tcp** command without specifying any parameters, the policy is created using the default values.

If the key (modulus) size is other than 512, 768, 1024, 1536, or 2048, you will receive an error and the trustpoint configuration is not applied. Replace the key by generating a key (using the same *key-label*) and specifying a supported modulus size, then reenter the name of the gateway that is used in the URL and the cookie mangling process using the **gateway-name** *gateway-name* command.

Examples

This example shows how to define the virtual gateway (this gateway is referenced in the WebVPN context) and enter the gateway submode:

```
webvpn(config)# webvpn gateway common
webvpn(config-webvpn-gateway)# ip address 172.21.65.71 port 443
webvpn(config-webvpn-gateway)# ssl trustpoint test.p12
webvpn(config-webvpn-gateway)# inservice
webvpn(config-webvpn-gateway)# end
webvpn#
```

webvpn policy ssl

To enter the SSL-policy configuration submode, use the **webvpn policy ssl** command. In the SSL-policy configuration submode, you can define the SSL policy for one or more SSL-proxy services.

webvpn policy ssl ssl-policy-name

Syntax Description

ssl-policy-name SSL policy name.

Defaults

The defaults are as follows:

- · cipher is all.
- · close-protocol is enabled.
- session-caching is enabled.
- · version is all.
- **session-cache size** *size* is 262143 entries.
- timeout session timeout is 0 seconds.
- timeout handshake timeout is 0 seconds.
- tls-rollback is disabled.

Command Modes

Global configuration

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

Each SSL-policy configuration submode command is entered on its own line.

Table 2-10 lists the commands available in SSL-policy configuration submode.

Table 2-10 SSL-Policy Configuration Submode Command Descriptions

cipher-suite {RSA_WITH_3DES_EDE_CBC_SHA RSA_WITH_DES_CBC_SHA RSA_WITH_RC4_128_MD5 RSA_WITH_RC4_128_SHA all}	Allows you to configure a list of cipher-suites acceptable to the proxy-server.
[no] close-protocol enable	Allows you to configure the SSL close-protocol behavior. Use the no form of this command to disable close protocol.
default {cipher close-protocol session-cache version}	Sets a command to its default settings.

Table 2-10 SSL-Policy Configuration Submode Command Descriptions (continued)

exit	Exits from SSL-policy configuration submode.		
help	Provides a description of the interactive help system.		
[no] session-cache enable	Allows you to enable the session-caching feature. Use the no form of this command to disable session-caching.		
session-cache size size	Specifies the maximum number of session entries to be allocated for a given service; valid values are from 1 to 262143 entries.		
timeout handshake timeout	Allows you to configure the amount of time that the module keeps the connection in handshake phase; valid values are from 0 to 65535 seconds.		
timeout session timeout [absolute]	Allows you to configure the session timeout. The syntax description is as follows:		
	• <i>timeout</i> —Session timeout; valid values are from 0 to 72000 seconds.		
	• absolute —(Optional) The session entry is not removed until the configured timeout has completed.		
tls-rollback [current any]	Allows you to specify if the SSL protocol version number in the TLS/SSL premaster secret message is either the maximum version or the negotiated version (current), or if the version is not checked (any).		
version {all ssl3 tls1}	Allows you to set the version of SSL to one of the following:		
	• all—Both SSL3 and TLS1 versions are used.		
	• ssl3—SSL version 3 is used.		
	• tls1—TLS version 1 is used.		

You can define the SSL policy templates using the **ssl-proxy policy ssl** *ssl-policy-name* command and associate an SSL policy with a particular proxy server using the proxy server configuration CLI. The SSL policy template allows you to define various parameters that are associated with the SSL handshake stack.

When you enable **close-notify**, a close-notify alert message is sent to the client and a close-notify alert message is expected from the client as well. When disabled, the server sends a close-notify alert message to the client; however, the server does not expect or wait for a close-notify message from the client before tearing down the session.

The cipher-suite names follow the same convention as the existing SSL stacks.

The cipher-suites that are acceptable to the proxy-server are as follows:

- RSA_WITH_3DES_EDE_CBC_SHA— RSA with 3des-sha
- RSA_WITH_DES_CBC_SHA—RSA with des-sha
- RSA_WITH_RC4_128_MD5—RSA with rc4-md5
- RSA_WITH_RC4_128_SHA—RSA with rc4-sha
- all—All supported ciphers

If you enter the **timeout session** *timeout* **absolute** command, the session entry is kept in the session cache for the configured timeout before it is cleaned up. If the session cache is full, the timers are active for all the entries, the **absolute** keyword is configured, and all further new sessions are rejected.

If you enter the **timeout session** *timeout* command without the **absolute** keyword, the specified timeout becomes the maximum timeout and a best-effort is made to keep the session entry in the session cache. If the session cache runs out of session entries, the session entry that is currently being used is removed for incoming new connections.

When you enter the **cert-req empty** command, the WebVPN Services Module backend service always returns the certificate associated with the trustpoint and does not look for CA-name match. By default, the WebVPN Services Module always looks for the CA-name match before returning the certificate. If the SSL server does not include a CA-name list in the certificate request during client authentication, the handshake fails.

By default, the WebVPN Services Module uses the maximum supported SSL protocol version (SSL2.0, SSL3.0, TLS1.0) in the ClientHello message. Enter the **tls-rollback** [**current** | **any**] command if the SSL client uses the negotiated version instead of the maximum supported version (as specified in the ClientHello message).

When you enter the **tls-rollback current** command, the SSL protocol version can be either the maximum supported version or the negotiated version.

When you enter the **tls-rollback any** command, the SSL protocol version is not checked at all.

Examples

This example shows how to enter the SSL-policy configuration submode:

```
wwbvpn(config)# webvpn policy ssl sslpl1
wwbvpn(config-ssl-policy)#
```

This example shows how to define the cipher suites that are supported for the SSL-policy:

```
wwbvpn(config-ssl-policy)# cipher RSA_WITH_3DES_EDE_CBC_SHA
wwbvpn(config-ssl-policy)#
```

This example shows how to enable the SSL session closing protocol:

```
wwbvpn(config-ssl-policy)# close-protocol enable
wwbvpn(config-ssl-policy)#
```

This example shows how to disable the SSL session closing protocol:

```
wwbvpn(config-ssl-policy)# no close-protocol enable
wwbvpn(config-ssl-policy)#
```

These examples shows how to set a specific command to its default setting:

```
wwbvpn(config-ssl-policy)# default cipher
wwbvpn(config-ssl-policy)# default close-protocol
wwbvpn(config-ssl-policy)# default session-cache
wwbvpn(config-ssl-policy)# default version
wwbvpn(config-ssl-policy)#
```

This example shows how to enable session-cache:

```
wwbvpn(config-ssl-policy)# session-cache enable
wwbvpn(config-ssl-policy)#
```

This example shows how to disable session-cache:

```
wwbvpn(config-ssl-policy)# no session-cache enable
wwbvpn(config-ssl-policy)#
```

This example shows how to set the maximum number of session entries to be allocated for a specific service:

```
wwbvpn(config-ssl-policy)# session-cache size 22000
wwbvpn(config-ssl-policy)#
```

This example shows how to configure the session timeout to absolute:

```
wwbvpn(config-ssl-policy)# timeout session 30000 absolute
wwbvpn(config-ssl-policy)#
```

These examples show how to enable the support of different SSL versions:

```
wwbvpn(config-ssl-policy)# version all
wwbvpn(config-ssl-policy)# version ssl3
wwbvpn(config-ssl-policy)# version tls1
wwbvpn(config-ssl-policy)#
```

This example shows how to print out a help page:

```
wwbvpn(config-ssl-policy)# help
wwbvpn(config-ssl-policy)#
```

Related Commands

show webvpn stats show webvpn stats ssl

webvpn policy tcp

To enter the proxy policy TCP configuration submode, use the **webvpn policy tcp** command. In proxy-policy TCP configuration submode, you can define the TCP policy templates.

webvpn policy tcp tcp-policy-name

Syntax Description

tcp-policy-name TCP policy name.

Defaults

The defaults are as follows:

- **buffer-share rx** is 32768 bytes.
- buffer-share tx is 32768 bytes.
- delayed-ack-threshold is 2 packets.
- delay-ack-timeout is 200 milliseconds.
- **mss** is 1460 bytes.
- nagle is enabled.
- timeout inactivity is 600 seconds.
- timeout fin-wait is 600 seconds.
- timeout syn is 75 seconds.
- timeout reassembly is 60 seconds.
- tos carryover is disabled.

Command Modes

Global configuration

Command History

Release	Modification
WebVPN Module Release 1.1	Support for this command was introduced on the Catalyst 6500 series switches.
Release 1.1	SWITCHES.

Usage Guidelines

After you define the TCP policy, you can associate the TCP policy with a proxy server using the proxy-policy TCP configuration submode commands.

Each proxy-policy TCP configuration submode command is entered on its own line.

Table 2-11 lists the commands that are available in proxy-policy TCP configuration submode.

Table 2-11 Proxy-policy TCP Configuration Submode Command Descriptions

default	Sets a command to its default settings.	
exit	Exits from proxy-service configuration submode.	

Table 2-11 Proxy-policy TCP Configuration Submode Command Descriptions (continued)

[no] buffer-share rx buffer-limit-in-bytes	Allows you to configure the maximum size of the receive buffer share per connection; valid values are from 8192 to 262144. Use the no form of this command to return to the default setting.			
[no] buffer-share tx buffer-limit-in-bytes	Allows you to configure the maximum size of the transmit buffer share per connection; valid values are from 8192 to 262144. Use the no form of this command to return to the default setting.			
delayed-ack-threshold	Allows you to specify the number of full-sized segments that must be received before a window-update ACK is sent. Valid values for packets are 1 to 10; the default value is 2.			
delay-ack-timeout	Allows you to specify the amount of time before a window-update ACK is sent.			
	If the number of full-sized segments (as specified in the delayed-ack-threshold command) is not received before this timer expires, then an ACK is sent acknowledging all data received up to this point, but the window is not updated. Valid values for timer are 50 to 500 milliseconds; the default value is 200.			
help	Provides a description of the interactive help system.			
[no] mss max-segment-size-in-bytes	Allows you to configure the maximum segment size that the connection identifies in the generated SYN packet; valid values are from 64 to 1460. Use the no form of this command to return to the default setting.			
[no] nagle	Allows you to enable the the Nagle algorithm.			
	When you enable the nagle keyword, small amounts of data that are written by the application is queued into the connection-send queue, but is not sent until one of the following situations occurs:			
	• There is data pending and an ACK arrives that acknowledges the data that was previously sent.			
	• The application writes more data so that a full-sized segment is created and sent.			
	When you disable the nagle keyword, queueing of data does not occur. All data that is written by the application is sent immediately.			
	Nagle is enabled by default.			
[no] timeout fin-wait timeout-in-seconds	Allows you to configure the FIN wait timeout; valid values are from 75 to 600 seconds. Use the no form of this command to return to the default setting.			
[no] timeout inactivity timeout-in-seconds	Allows you to configure the inactivity timeout; valid values are from 0 to 960 seconds. This command allows you to set the aging timeout for an idle connection and helps protect the connection resources. Use the no form of this command to return to the default setting.			
[no] timeout syn timeout-in-seconds	Allows you to configure the connection establishment timeout; valid values are from 5 to 75 seconds. Use the no form of this command to return to the default setting.			

Table 2-11 Proxy-policy TCP Configuration Submode Command Descriptions (continued)

[no] timeout reassembly time	Allows you to configure the amount of time in seconds before the reassembly queue is cleared; valid values are from 0 to 960 seconds (0 = disabled). If the transaction is not complete within the specified time, the reassembly queue is cleared and the connection is dropped. Use the no form of this command to return to the default setting.		
[no] tos carryover	Forwa Note	If the policy is configured as a server TCP policy, the ToS value is sent from the server to the client. If the policy is configured as a virtual policy, the ToS value is sent from the server.	
	Note	The ToS value needs to be learned before it can be propagated. For example, when a ToS value is configured to be propagated from the server to client connection, the server connection must be established before the value is learned and propagated. Therefore, some of the initial packets will not carry the ToS value.	

Usage Guidelines

TCP commands that you enter on the WebVPN Services Module can apply either globally or to a particular proxy server.

You can configure a different maximum segment size for the client side and the server side of the proxy server.

The TCP policy template allows you to define parameters that are associated with the TCP stack.

You can either enter the **no** form of the command or use the **default** keyword to return to the default setting.

Examples

This example shows how to enter the proxy-policy TCP configuration submode:

```
wwbvpn(config)# webvpn policy tcp tcppl1
wwbvpn(config-tcp-policy)#
```

These examples show how to set a given command to its default value:

```
wwbvpn(config-tcp-policy)# default timeout fin-wait
wwbvpn(config-tcp-policy)# default inactivity-timeout
wwbvpn(config-tcp-policy)# default buffer-share rx
wwbvpn(config-tcp-policy)# default buffer-share tx
wwbvpn(config-tcp-policy)# default mss
wwbvpn(config-tcp-policy)# default timeout syn
wwbvpn(config-tcp-policy)#
```

This example shows how to define the FIN-wait timeout in seconds:

```
wwbvpn(config-tcp-policy)# timeout fin-wait 200
wwbvpn(config-tcp-policy)#
```

This example shows how to define the inactivity timeout in seconds:

```
wwbvpn(config-tcp-policy)# timeout inactivity 300
wwbvpn(config-tcp-policy)#
```

This example shows how to define the maximum size for the receive buffer configuration:

```
wwbvpn(config-tcp-policy)# buffer-share rx 16384
```

```
wwbvpn(config-tcp-policy)#
```

This example shows how to define the maximum size for the transmit buffer configuration:

```
wwbvpn(config-tcp-policy)# buffer-share tx 13444
wwbvpn(config-tcp-policy)#
```

This example shows how to define the maximum size for the TCP segment:

```
wwbvpn(config-tcp-policy)# mss 1460
wwbvpn(config-tcp-policy)#
```

This example shows how to define the initial connection (SYN)-timeout value:

```
wwbvpn(config-tcp-policy)# timeout syn 5
wwbvpn(config-tcp-policy)#
```

This example shows how to define the reassembly-timeout value:

```
wwbvpn(config-tcp-policy)# timeout reassembly 120
wwbvpn(config-tcp-policy)#
```

This example shows how to enable carryover the ToS value to all packets within a flow:

```
wwbvpn(config-tcp-policy)# tos carryover
wwbvpn(config-tcp-policy)#
```

Related Commands

show webvpn policy

webvpn policy tcp